II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSER

RÅDETS AFGØRELSE

af 31. marts 2011

om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer

(2011/292/EU)

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 240, stk. 3,

under henvisning til Rådets afgørelse 2009/937/EU af 1. december 2009 om vedtagelse af Rådets forretningsorden [1], særlig artikel 24, og

ud fra følgende betragtninger:

(1) For at udbygge Rådets virksomhed på alle områder, som kræver håndtering af klassificerede informationer, er det hensigtsmæssigt at indføre et overordnet system for sikkerhedsbeskyttelse af klassificerede informationer, der omfatter Rådet, Rådets Generalsekretariat og medlemsstaterne.

(2) Denne afgørelse bør finde anvendelse, når Rådet, dets forberedende organer og Generalsekretariatet for Rådet (GSR) håndterer EU's klassificerede informationer (EUCI).

(3) I overensstemmelse med nationale love og bestemmelser og i det omfang, det er nødvendigt for Rådets funktion, bør medlemsstaterne overholde denne afgørelse, når deres kompetente myndigheder, personale eller kontrahenter håndterer EUCI, så de hver især kan være sikre på, at der gælder et ækvivalent beskyttelsesniveau for EUCI.

(4) Rådet og Kommissionen er fast besluttet på at anvende ækvivalente sikkerhedsstandarder for beskyttelse af EUCI.

(5) Rådet understreger vigtigheden af, at Europa-Parlamentet og andre EU-institutioner, -agenturer, -organer eller -kontorer, når det er relevant, omfattes af de principper, standarder og regler for sikkerhedsbeskyttelse af klassificerede informationer, der er nødvendige for at beskytte Unionens og dens medlemsstaters interesser.

(6) EU-agenturer og -organer oprettet i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union anvender Europol og Eurojust i deres interne organisation de grundprincipper og minimumsstandarder, der er fastlagt i denne afgørelse med henblik på sikkerhedsbeskyttelse af EUCI, jf. deres respektive grundlæggende akter.

(7) Krisestyringsoperationer etableret i henhold til afsnit V, kapitel 2 i traktaten om Den Europæiske Union og deres personale anvender de regler, der er vedtaget af Rådet med henblik på sikkerhedsbeskyttelse af EUCI.

(8) EU's særlige repræsentanter og medlemmerne af deres stab anvender de regler, der er vedtaget af Rådet med henblik på sikkerhedsbeskyttelse af EUCI.

(9) Denne afgørelse gælder med forbehold af artikel 15 og 16 i traktaten om Den Europæiske Unions funktionsmåde og retsakter til gennemførelse heraf.

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

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Formål, anvendelsesområde og definitioner

1. Denne afgørelse fastlægger grundprincipperne og minimumsstandarderne for sikkerhedsbeskyttelse af EUCI.

[1] EUT L 325 af 11.12.2009, s. 35.

2. Disse grundprincipper og minimumsstandarder gælder for Rådet og GSR og skal overholdes af medlemsstaterne i overensstemmelse med deres respektive nationale love og bestemmelser, så de hver især kan være sikre på, at der gælder et ækvivalent beskyttelsesniveau for EUCI.

3. I denne afgørelse anvendes de definitioner, der er fastlagt i tillæg A.

Artikel 2

Definition af EUCI, sikkerhedsklassifikationer og mærkninger

1. Ved »EU's klassificerede informationer« (EUCI) forstås informationer eller materiale mærket med en EU-sikkerhedsklassifikation, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes interesser skade i forskellig grad.

2. EUCI klassificeres efter en af følgende grader:

a) TRÈS SECRET UE/EU TOP SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser overordentlig alvorlig skade.

b) SECRET UE/EU SECRET: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser alvorlig skade.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informationer og materiale, hvis uautoriserede videregivelse kunne forvolde Den Europæiske Unions eller en eller flere af medlemsstaternes væsentlige interesser skade.

d) RESTREINT UE/EU RESTRICTED: informationer og materiale, hvis uautoriserede videregivelse kunne have negativ indvirkning på Den Europæiske Unions eller en eller flere af medlemsstaternes interesser.

3. EUCI forsynes med en klassifikationsmærkning i overensstemmelse med stk. 2. EUCI kan forsynes med yderligere mærkninger for at angive de aktivitetsområder, de vedrører, identificere udstederen, begrænse distributionen eller anvendelsen eller angive mulighederne for videregivelse.

Artikel 3

Klassifikationsstyring

1. De kompetente myndigheder sikrer, at EUCI er passende klassificeret, klart identificeret som klassificerede informationer og kun bevarer deres klassifikationsgrad, så længe det er nødvendigt.

2. EUCI må ikke nedklassificeres eller afklassificeres, og ingen af mærkningerne ifølge artikel 2, stk. 3, må ændres eller fjernes uden forudgående skriftligt samtykke fra udstederen.

3. Rådet godkender en sikkerhedspolitik for udarbejdelse af EUCI, der omfatter en praktisk klassifikationsvejledning.

Artikel 4

Beskyttelse af klassificerede informationer

1. EUCI beskyttes i overensstemmelse med denne afgørelse.

2. Den, der er i besiddelse af EUCI, er ansvarlig for beskyttelse heraf i overensstemmelse med denne afgørelse.

3. Hvis medlemsstaterne bringer klassificerede informationer med en national klassifikationsmærkning ind i Den Europæiske Unions strukturer eller netværk, beskytter Rådet og GSR disse informationer i overensstemmelse med de krav, der gælder for EUCI af en tilsvarende grad, jf. den sammenlignende oversigt over sikkerhedsklassifikationer i tillæg B.

4. Større mængder eller en samling af EUCI kan berettige til en sikkerhedsbeskyttelse af en grad, der svarer til en højere klassifikation.

Artikel 5

Sikkerhedsrisikostyring

1. Risici i forhold til EUCI skal styres som en proces. Processen har til formål at fastslå kendte sikkerhedsrisici, fastlægge sikkerhedsforanstaltninger for at reducere sådanne risici til et acceptabelt niveau i overensstemmelse med de grundprincipper og minimumsstandarder, der er fastlagt i denne afgørelse, og anvende disse foranstaltninger ifølge begrebet dybdeforsvar, jf. definitionen i tillæg A. Sådanne foranstaltningers effektivitet skal løbende evalueres.

2. Sikkerhedsforanstaltninger til beskyttelse af EUCI i hele deres livscyklus skal især svare til sikkerhedsklassifikationen for og formen og mængden af informationerne eller materialet, placeringen og konstruktionen af de faciliteter, hvor EUCI opbevares, og den lokalt vurderede trussel fra ondsindet og/eller kriminel virksomhed, herunder spionage, sabotage og terrorisme.

3. Beredskabsplaner skal tage hensyn til behovet for at beskytte EUCI i nødsituationer med henblik på at forhindre uautoriseret adgang, uautoriseret videregivelse eller tab af integritet eller tilgængelighed.

4. Kontinuitetsplaner skal omfatte forebyggende og genoprettende foranstaltninger med henblik på at minimere følgerne af større nedbrud eller hændelser for håndteringen og opbevaringen af EUCI.

Artikel 6

Gennemførelse af denne afgørelse

1. Når det er nødvendigt, godkender Rådet efter henstilling fra Sikkerhedsudvalget sikkerhedspolitikker med foranstaltninger til gennemførelse af denne afgørelse.

2. Sikkerhedsudvalget kan på sit niveau fastlægge sikkerhedsretningslinjer for at supplere eller understøtte denne afgørelse og eventuelle sikkerhedspolitikker, der er godkendt af Rådet.

Artikel 7

Personelsikkerhed

1. Ved personelsikkerhed forstås anvendelse af foranstaltninger for at sikre, at adgang til EUCI kun gives til personer, som:

— har need-to-know

— er sikkerhedsgodkendt til den relevante klassifikationsgrad, når det er nødvendigt, og

— er blevet gjort bekendt med deres ansvar.

2. Procedurerne for personelsikkerhedsgodkendelse udformes, så det kan afgøres, om en person under hensyn til vedkommendes loyalitet, troværdighed og pålidelighed kan autoriseres til at få adgang til EUCI.

3. Alle personer i GSR, hvis opgaver kan kræve adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal være sikkerhedsgodkendt til den relevante klassifikationsgrad, inden de kan få adgang til sådanne EUCI. Proceduren for personelsikkerhedsgodkendelse for GSR's tjenestemænd og øvrige ansatte er fastlagt i bilag I.

4. Medlemsstaternes personale, jf. artikel 14, stk. 3, hvis opgaver kan kræve adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal være sikkerhedsgodkendt til den relevante klassifikationsgrad eller på anden måde behørigt autoriseret i kraft af deres funktioner i overensstemmelse med nationale love og bestemmelser, inden de kan få adgang til sådanne EUCI.

5. Alle personer skal gøres bekendt med og anerkende deres ansvar for at beskytte EUCI i overensstemmelse med denne afgørelse, inden de får adgang til EUCI og med jævne mellemrum herefter.

6. Bestemmelser til gennemførelse af denne artikel findes i bilag I.

Artikel 8

Fysisk sikkerhed

1. Ved fysisk sikkerhed forstås anvendelse af fysiske og tekniske beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til EUCI.

2. De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre, at en indtrænger skaffer sig hemmelig adgang eller tiltvinger sig adgang, på at afskrække fra, vanskeliggøre og afsløre uautoriserede handlinger samt på at muliggøre personalemæssig adskillelse for så vidt angår adgang til EUCI på en need-to-know-basis. Sådanne foranstaltninger fastlægges på basis af en risikostyringsproces.

3. Fysiske sikkerhedsforanstaltninger indføres for alle lokaliteter, bygninger, kontorer, lokaler og andre områder, hvor EUCI håndteres eller opbevares, herunder områder, der huser kommunikations- og informationssystemer, jf. artikel 10, stk. 2.

4. Områder, hvor EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, opbevares, skal etableres som sikrede områder i overensstemmelse med bilag II og godkendes af den kompetente sikkerhedsmyndighed.

5. Der må kun anvendes godkendt udstyr eller godkendte anordninger til beskyttelse af EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere.

6. Bestemmelser til gennemførelse af denne artikel findes i bilag II.

Artikel 9

Forvaltning af klassificerede informationer

1. Ved forvaltning af klassificerede informationer forstås anvendelse af administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus for at supplere foranstaltningerne i artikel 7, 8 og 10 og derved bidrage til at afskrække fra, afsløre og udbedre skade forårsaget af forsætlig eller uagtsom kompromittering eller tab af sådanne informationer. Sådanne foranstaltninger omfatter bl.a. udarbejdelse, registrering, kopiering, oversættelse, transport og destruktion af EUCI.

2. Informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, sikkerhedsregistreres forud for distributionen og ved modtagelsen. GSR's og medlemsstaternes respektive kompetente myndigheder etablerer en registraturordning med henblik herpå. Informationer, der er klassificeret TRES SECRET UE/EU TOP SECRET, registreres i dertil oprettede registraturer.

3. Tjenester og lokaliteter, hvor EUCI håndteres eller opbevares, underkastes regelmæssig inspektion af den kompetente sikkerhedsmyndighed.

4. EUCI transporteres på følgende måde mellem tjenester og lokaliteter uden for fysisk beskyttede områder:

a) generelt ved elektronisk transmission beskyttet af kryptoprodukter, der er godkendt i overensstemmelse med artikel 10, stk. 6

b) når de i litra a) omhandlede midler ikke anvendes, transporteres EUCI enten:

i) via elektroniske medier (f.eks. USB-nøgler, CD'er og harddiske) beskyttet af kryptoprodukter, der er godkendt i overensstemmelse med artikel 10, stk. 6, eller

ii) i alle andre tilfælde som foreskrevet af den kompetente sikkerhedsmyndighed i overensstemmelse med de relevante beskyttelsesforanstaltninger i bilag III.

5. Bestemmelser til gennemførelse af denne artikel findes i bilag III.

Artikel 10

Beskyttelse af EUCI, der håndteres i kommunikations- og informationssystemer

1. Ved informationssikring (IA) i forbindelse med kommunikations- og informationssystemer forstås tilliden til, at disse systemer beskytter de informationer, de håndterer, og at de fungerer, som de skal, når de skal, under de legitime brugeres kontrol. Effektiv IA sikrer et passende niveau af fortrolighed, integritet, tilgængelighed, uafviselighed og autenticitet. IA baseres på en risikostyringsproces.

2. Ved »kommunikations- og informationssystem« forstås et system, der muliggør håndtering af informationer i elektronisk form. Et kommunikations- og informationssystem omfatter alle de aktiver, der er nødvendige for dets drift, herunder infrastrukturer, organisation, personale og informationsressourcer. Denne afgørelse finder anvendelse på kommunikations- og informationssystemer, der håndterer EUCI (CIS'er).

3. CIS'er håndterer EUCI i overensstemmelse med begrebet IA.

4. Alle CIS'er skal gennemgå en akkrediteringsproces. Akkreditering har til formål at sikre, at alle passende sikkerhedsforanstaltninger er blevet gennemført, og at der er opnået en tilstrækkelig grad af beskyttelse af EUCI og af CIS'et i overensstemmelse med denne afgørelse. Akkrediteringsudredningen skal fastsætte den højeste klassifikationsgrad af de informationer, der kan håndteres i et CIS, og de betingelser og vilkår, der svarer hertil.

5. CIS'er, der håndterer informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal sikkerhedsbeskyttes, således at informationerne ikke kan kompromitteres gennem utilsigtede elektromagnetiske emissioner (Tempestsikkerhedsforanstaltninger).

6. Hvis beskyttelsen af EUCI sker ved hjælp af kryptoprodukter, skal sådanne produkter være godkendt på følgende måde:

a) fortroligheden af informationer, der er klassificeret SECRET UE/EU SECRET eller højere, skal beskyttes ved hjælp af kryptoprodukter, der er godkendt af Rådet som kryptogodkendelsesmyndighed (CAA) efter henstilling fra Sikkerhedsudvalget

b) fortroligheden af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED, skal beskyttes ved hjælp af kryptoprodukter, der er godkendt af generalsekretæren for Rådet (i det følgende benævnt »generalsekretæren«) som CAA efter henstilling fra Sikkerhedsudvalget.

Uanset litra b) kan fortroligheden af EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED, inden for medlemsstaternes nationale systemer beskyttes ved hjælp af kryptoprodukter, der er godkendt af en medlemsstats CAA.

7. Ved elektronisk transmission af EUCI skal der anvendes godkendte kryptoprodukter. Uanset dette krav kan der i nødsituationer følges specifikke procedurer eller anvendes specifikke tekniske konfigurationer, jf. bilag IV.

8. GSR's og medlemsstaternes respektive kompetente myndigheder etablerer følgende IA-funktioner:

a) en IA-myndighed (IAA)

b) en Tempestmyndighed (TA)

c) en kryptogodkendelsesmyndighed (CAA)

d) en kryptodistributionsmyndighed (CDA).

9. For hvert system etablerer GSR's og medlemsstaternes respektive kompetente myndigheder:

a) en sikkerhedsakkrediteringsmyndighed (SAA)

b) en operativ IA-myndighed.

10. Bestemmelser til gennemførelse af denne artikel findes i bilag IV.

Artikel 11

Industrisikkerhed

1. Ved industrisikkerhed forstås anvendelse af foranstaltninger for at sikre, at kontrahenter eller underkontrahenter beskytter EUCI under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter. Sådanne kontrakter må ikke indebære adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET.

2. GSR kan ved aftale overdrage opgaver, som indebærer eller medfører adgang til eller håndtering eller opbevaring af EUCI, til industrivirksomheder eller andre enheder, som er registreret i en medlemsstat eller i et tredjeland, der har indgået en aftale eller en administrativ ordning i henhold til artikel 12, stk. 2, litra a) eller b).

3. GSR sikrer som kontraherende myndighed, at minimumsstandarderne for industrisikkerhed som fastlagt i denne afgørelse og omhandlet i kontrakten overholdes, når der tildeles klassificerede kontrakter til industrivirksomheder eller andre enheder.

4. Den nationale sikkerhedsmyndighed (NSA), den udpegede sikkerhedsmyndighed (DSA) eller en hvilken som helst anden kompetent myndighed i den enkelte medlemsstat sikrer, så vidt det er muligt i henhold til nationale love og bestemmelser, at kontrahenter og underkontrahenter, der er registreret på deres område, træffer alle relevante foranstaltninger til at beskytte EUCI under forhandlingerne forud for indgåelsen af en kontrakt og under opfyldelsen af en klassificeret kontrakt.

5. NSA'en, DSA'en eller en hvilken som helst anden kompetent sikkerhedsmyndighed i den enkelte medlemsstat sikrer i overensstemmelse med nationale love og bestemmelser, at kontrahenter eller underkontrahenter, der er registreret i den pågældende medlemsstat og deltager i klassificerede kontrakter eller underkontrakter, som kræver adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET inden for deres faciliteter, enten i forbindelse med opfyldelsen af kontrakterne eller i perioden forud for indgåelsen af kontrakterne, er i besiddelse af en facilitetssikkerhedsgodkendelse (FSC) til den krævede klassifikationsgrad.

6. En kontrahents eller underkontrahents personale, der med henblik på opfyldelse af en klassificeret kontrakt skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal tildeles en personelsikkerhedsgodkendelse (PSC) af den pågældende NSA eller DSA eller anden kompetent sikkerhedsmyndighed i overensstemmelse med nationale love og bestemmelser og de minimumsstandarder, der er fastlagt i bilag I.

7. Bestemmelserne til gennemførelse af denne artikel findes i bilag V.

Artikel 12

Udveksling af klassificerede informationer med tredjelande og internationale organisationer

1. Hvis Rådet beslutter, at det er nødvendigt at udveksle EUCI med et tredjeland eller en international organisation, etableres der passende rammer herfor.

2. For at etablere sådanne rammer og definere gensidige regler for sikkerhedsbeskyttelse af de klassificerede informationer, der udveksles,

a) skal Rådet indgå aftaler om sikkerhedsprocedurer for udveksling og beskyttelse af klassificerede informationer (informationssikkerhedsaftaler) eller

b) kan generalsekretæren indgå administrative ordninger herom i overensstemmelse med bilag VI, punkt 17, hvis klassifikationsgraden for de EUCI, der skal videregives, generelt ikke er højere end RESTREINT UE/EU RESTRICTED.

3. Informationssikkerhedsaftaler eller administrative ordninger, jf. stk. 2, skal indeholde bestemmelser, der sikrer, at tredjelande eller internationale organisationer, når de modtager EUCI, sikkerhedsbeskytter sådanne informationer i overensstemmelse med informationernes klassifikationsgrad og efter minimumsstandarder, som mindst svarer til de standarder, der er fastlagt i denne afgørelse.

4. Beslutningen om at videregive EUCI, der er udfærdiget i Rådet, til et tredjeland eller en international organisation, træffes af Rådet fra sag til sag på grundlag af informationernes art og indhold, modtagerens need-to-know og EU's interesse i videregivelsen. Hvis udstederen af de klassificerede informationer, der ønskes videregivet, ikke er Rådet, skal GSR først indhente udstederens skriftlige samtykke til videregivelsen. Hvis det ikke kan fastslås, hvem udstederen er, påtager Rådet sig dennes ansvar.

5. Der foretages vurderingsbesøg for at konstatere effektiviteten af de foranstaltninger, der gælder i et tredjeland eller en international organisation med henblik på sikkerhedsbeskyttelse af EUCI, der videregives eller udveksles.

6. Bestemmelser til gennemførelse af denne artikel findes i bilag VI.

Artikel 13

Brud på sikkerheden og kompromittering af EUCI

1. Ved brud på sikkerheden forstås resultatet af en persons handling eller forsømmelse, der er i strid med sikkerhedsreglerne i denne afgørelse.

2. EUCI anses for at være kompromitteret, hvis de som følge af et brud på sikkerheden helt eller delvist er videregivet til uautoriserede personer.

3. Eventuelle brud på eller eventuel mistanke om brud på sikkerheden skal straks meldes til den kompetente sikkerhedsmyndighed.

4. Hvis det konstateres, eller hvis der er rimelig grund til at formode, at EUCI er kompromitteret eller bortkommet, skal den kompetente sikkerhedsmyndighed træffe alle passende foranstaltninger i overensstemmelse med de relevante love og bestemmelser for at:

a) orientere udstederen

b) sikre, at sagen undersøges af personale, der ikke er direkte involveret i bruddet på sikkerheden, for at fastslå de faktiske omstændigheder

c) vurdere den potentielle skade for EU's eller medlemsstaternes interesser

d) træffe passende foranstaltninger til at forebygge en gentagelse og

e) underrette de relevante myndigheder om de foranstaltninger, der er truffet.

5. Enhver, der er ansvarlig for brud på sikkerhedsreglerne i denne afgørelse, kan pålægges disciplinære foranstaltninger i overensstemmelse med gældende regler og bestemmelser. Enhver, der er ansvarlig for kompromittering eller bortkomst af EUCI, pålægges disciplinære foranstaltninger og/eller retsforfølges i overensstemmelse med gældende love, regler og bestemmelser.

Artikel 14

Ansvar for gennemførelsen

1. Rådet træffer alle nødvendige foranstaltninger for at sikre overordnet sammenhæng i anvendelsen af denne afgørelse.

2. Generalsekretæren træffer alle nødvendige foranstaltninger for i forbindelse med håndtering eller opbevaring af EUCI eller andre klassificerede informationer at sikre, at denne afgørelse anvendes i lokaliteter, der benyttes af Rådet, og inden for GSR, herunder i dets forbindelseskontorer i tredjelande, og af GSR's tjenestemænd og øvrige ansatte, af personale, som er udstationeret ved GSR, og af GSR's kontrahenter.

3. Medlemsstaterne træffer i overensstemmelse med deres respektive nationale love og bestemmelser alle passende foranstaltninger for i forbindelse med håndtering eller opbevaring af EUCI at sikre, at denne afgørelse overholdes af:

a) personalet ved medlemsstaternes faste repræsentationer ved Den Europæiske Union og nationale delegerede, der deltager i møder i Rådet eller i dets forberedende organer eller i andre rådsaktiviteter

b) andet personale i medlemsstaternes nationale administrationer, herunder personale, som er udstationeret ved disse administrationer, uanset om de pågældende gør tjeneste på medlemsstaternes område eller i udlandet

c) andre personer i medlemsstaterne, der i kraft af deres funktioner er behørigt autoriseret til at have adgang til EUCI, og

d) medlemsstaternes kontrahenter, uanset om de befinder sig på medlemsstaternes område eller i udlandet.

Artikel 15

Sikkerhedsorganisation i Rådet

1. Som led i sin rolle med hensyn til at sikre overordnet sammenhæng i anvendelsen af denne afgørelse godkender Rådet:

a) de aftaler, der er omhandlet i artikel 12, stk. 2, litra a)

b) beslutninger om videregivelse af EUCI til tredjelande og internationale organisationer

c) et årligt inspektionsprogram foreslået af generalsekretæren og anbefalet af Sikkerhedsudvalget med henblik på inspektion af medlemsstaternes tjenester og lokaliteter, af EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union og af Europol og Eurojust, samt vurderingsbesøg til tredjelande og internationale organisationer for at konstatere effektiviteten af de foranstaltninger, der gennemføres for at sikkerhedsbeskytte EUCI, og

d) sikkerhedspolitikker som omhandlet i artikel 6, stk. 1.

2. Generalsekretæren er GSR's sikkerhedsmyndighed. Generalsekretæren skal i den egenskab:

a) gennemføre Rådets sikkerhedspolitik og løbende tage den op til revision

b) med medlemsstaternes NSA'er koordinere alle spørgsmål vedrørende sikkerhedsbeskyttelse af klassificerede informationer, som er relevante for Rådets aktiviteter

c) tildele EU-PSC'er til GSR's tjenestemænd og øvrige ansatte i overensstemmelse med artikel 7, stk. 3, inden de kan få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere

d) når det er relevant, iværksætte undersøgelser ved konstatering af eller mistanke om kompromittering eller tab af klassificerede informationer, som er i Rådets besiddelse eller er udfærdiget af Rådet, og anmode de relevante sikkerhedsmyndigheder om at bistå med sådanne undersøgelser

e) iværksætte periodiske inspektioner af ordningerne for sikkerhedsbeskyttelse af klassificerede informationer i GSR's lokaliteter

f) iværksætte periodiske inspektioner af ordningerne for sikkerhedsbeskyttelse af EUCI i EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union, i Europol og Eurojust samt i krisestyringsoperationer etableret i henhold til afsnit V, kapitel 2 i traktaten om Den Europæiske Union og hos EU's særlige repræsentanter (EUSR) og medlemmerne af deres stab

g) sammen med og i forståelse med de pågældende NSA'er iværksætte periodiske inspektioner af ordningerne for sikkerhedsbeskyttelse af EUCI i medlemsstaternes tjenester og lokaliteter

h) koordinere sikkerhedsforanstaltninger med de kompetente myndigheder i medlemsstaterne, der er ansvarlige for sikkerhedsbeskyttelse af klassificerede informationer, og, når det er relevant, i tredjelande eller internationale organisationer, bl.a. om arten af trusler mod EUCI's sikkerhed og midlerne til beskyttelse mod dem

i) indgå de administrative ordninger, der er omhandlet i artikel 12, stk. 2, litra b), og

j) foretage indledende og periodiske vurderingsbesøg til tredjelande eller internationale organisationer for at konstatere effektiviteten af de foranstaltninger, der gennemføres for at sikkerhedsbeskytte EUCI, der videregives til eller udveksles med dem.

GSR's Sikkerhedskontor står til rådighed for generalsekretæren for at bistå ham med disse ansvarsområder.

3. Med henblik på anvendelsen af artikel 14, stk. 3, bør medlemsstaterne:

a) udpege en NSA, der er ansvarlig for ordningerne for sikkerhedsbeskyttelse af EUCI, således at

   i) EUCI, der opbevares af nationale styrelser, organer eller agenturer, offentlige eller private, i ind- eller udland, er sikkerhedsbeskyttet i overensstemmelse med denne afgørelse

   ii) ordningerne for sikkerhedsbeskyttelse af EUCI inspiceres med jævne mellemrum

   iii) alle personer, der er ansat i en national myndighed eller af en kontrahent, og som kan få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, er behørigt sikkerhedsgodkendt eller på anden måde i kraft af deres funktioner er behørigt autoriseret i overensstemmelse med nationale love og bestemmelser

   iv) der indføres de nødvendige sikkerhedsprogrammer for at minimere risikoen for, at EUCI kompromitteres eller bortkommer

   v) spørgsmål vedrørende sikkerhedsbeskyttelse af EUCI koordineres med andre kompetente nationale myndigheder, herunder dem, der er omhandlet i denne afgørelse, og

   vi) der reageres på relevante anmodninger om sikkerhedsgodkendelse fra EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union, fra Europol og Eurojust samt fra krisestyringsoperationer etableret i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union og fra EUSR'er og deres stab.

   Der findes en liste over NSA'er i tillæg C.

b) sikre, at deres kompetente myndigheder underretter og rådgiver deres regeringer og derigennem Rådet om arten af trusler mod EUCI's sikkerhed og midlerne til beskyttelse mod dem.

Artikel 16

Sikkerhedsudvalget

1. Der nedsættes et sikkerhedsudvalg. Det undersøger og vurderer sikkerhedsspørgsmål inden for rammerne af denne afgørelse og fremsætter henstillinger til Rådet, når det er relevant.

2. Sikkerhedsudvalget består af repræsentanter for medlemsstaternes NSA'er med deltagelse af en repræsentant for Kommissionen og for Tjenesten for EU's Optræden Udadtil. Udvalget ledes af generalsekretæren eller en af denne udpeget delegeret. Det træder sammen efter Rådets anvisninger eller på anmodning af generalsekretæren eller af en NSA.

Repræsentanter for EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union samt Europol og Eurojust kan indbydes til at deltage, når der drøftes spørgsmål, som vedrører dem.

3. Sikkerhedsudvalget tilrettelægger sine aktiviteter, så det kan fremsætte henstillinger om specifikke sikkerhedsområder. Det nedsætter ekspertundergrupper for IA-spørgsmål og andre ekspertundergrupper, når det er nødvendigt. Det udarbejder mandater for sådanne ekspertundergrupper og modtager rapporter fra dem om deres virksomhed, herunder henstillinger til Rådet, når det er relevant.

Artikel 17

Ophævelse af tidligere afgørelse

1. Denne afgørelse ophæver og træder i stedet for afgørelse 2001/264/EF af 19. marts 2001 om vedtagelse af Rådets sikkerhedsforskrifter ([1]).

2. Alle EUCI, der er klassificeret i overensstemmelse med Rådets afgørelse 2001/264/EF, sikkerhedsbeskyttes fortsat i overensstemmelse med de relevante bestemmelser i nærværende afgørelse.

Artikel 18

Ikrafttræden

Denne afgørelse træder i kraft dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 31. marts 2011.

På Rådets vegne
VÖLNER P.
Formand

([1]) EFT L 101 af 11.4.2001, s. 1.

BILAG

BILAG I

Personelsikkerhed

BILAG II

Fysisk sikkerhed

BILAG III

Forvaltning af klassificerede informationer

BILAG IV

Beskyttelse af EUCI, der håndteres i CIS'er

BILAG V

Industrisikkerhed

BILAG VI

Udveksling af klassificerede informationer med tredjelande og internationale organisationer

BILAG I

PERSONELSIKKERHED

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 7. Det fastsætter navnlig kriterierne for fastlæggelse af, om en person under hensyntagen til vedkommendes loyalitet, troværdighed og pålidelighed kan autoriseres til at få adgang til EUCI, samt de undersøgelsesmæssige og administrative procedurer, der skal følges i den forbindelse.

2. I dette bilag henviser begrebet »personelsikkerhedsgodkendelse«til en national personelsikkerhedsgodkendelse (national PSC) og/eller en EU-personelsikkerhedsgodkendelse (EU-PSC) som defineret i tillæg A.

II. AUTORISATION TIL AT FÅ ADGANG TIL EUCI

3. En person kan kun autoriseres til at få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, efter at:

   a) vedkommendes need-to-know er fastslået

   b) den pågældende har fået en PSC til den relevante grad eller på anden vis i kraft af sine funktioner er behørigt autoriseret i overensstemmelse med nationale love og bestemmelser, og

   c) den pågældende er blevet gjort bekendt med regler og procedurer for sikkerhedsbeskyttelse af EUCI og har anerkendt sit ansvar med hensyn til beskyttelse af sådan informationer.

4. Hver medlemsstat og GSR identificerer de stillinger i deres struktur, der kræver adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, og hvortil der derfor kræves en PSC til den relevante klassifikationsgrad.

III. KRAV TIL PERSONELSIKKERHEDSGODKENDELSE

5. Efter at have modtaget en behørigt autoriseret anmodning er NSA'er eller andre kompetente nationale myndigheder ansvarlige for at sikre, at der gennemføres sikkerhedsundersøgelser af egne statsborgere, der skal have adgang til informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere. Standarderne for undersøgelserne skal være i overensstemmelse med nationale love og bestemmelser.

6. Såfremt den pågældende person har sin bopæl på en anden medlemsstats eller et tredjelands område, anmoder de kompetente nationale myndigheder om bistand fra den kompetente myndighed i bopælslandet i overensstemmelse med nationale love og bestemmelser. Medlemsstaterne bistår hinanden med gennemførelsen af sikkerhedsundersøgelserne i overensstemmelse med nationale love og bestemmelser.

7. Hvis der er hjemmel herfor i nationale love og bestemmelser, kan NSA'er eller andre kompetente nationale myndigheder gennemføre undersøgelser af ikke-statsborgere, der skal have adgang til informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere. Standarderne for undersøgelserne skal være i overensstemmelse med nationale love og bestemmelser.

Kriterier for sikkerhedsundersøgelse

8. For at fastslå en persons loyalitet, troværdighed og pålidelighed med henblik på tildeling af en PSC for adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, foretages en sikkerhedsundersøgelse. Den kompetente nationale myndighed foretager en overordnet vurdering på grundlag af resultaterne af en sådan sikkerhedsundersøgelse. Et enkelt negativt resultat udgør ikke nødvendigvis en grund til at nægte en PSC. De væsentlige kriterier, der anvendes hertil, bør omfatte, så vidt det er muligt i henhold til nationale love og bestemmelser, en undersøgelse af, om personen:

   a) har begået eller forsøgt at begå spionage, terrorisme, sabotage, forræderi eller oprør, eller har konspireret med eller hjulpet eller tilskyndet en anden til at begå sådanne handlinger

   b) har eller har haft forbindelse med spioner, terrorister, sabotører eller med personer, der med rimelighed kan mistænkes for at være det, eller forbindelse med repræsentanter for organisationer eller fremmede stater, herunder fremmede efterretningstjenester, der kan udgøre en sikkerhedsrisiko for EU og/eller medlemsstater, medmindre de pågældende forbindelser var autoriseret som led i tjenesten

c) er eller har været medlem af en organisation, som med voldelige, undergravende eller andre ulovlige midler bl.a. søger at styrte regeringen i en medlemsstat, at ændre en medlemsstats forfatningsmæssige orden eller dens regeringsform eller -politik

d) støtter eller har støttet en af de i litra c) beskrevne organisationer eller har haft nær tilknytning til medlemmer af sådanne organisationer

e) bevidst har tilbageholdt, forvansket eller forfalsket vigtige oplysninger, navnlig af sikkerhedsmæssig art, eller har afgivet bevidst urigtige oplysninger ved udfyldelsen af et spørgeskema om personelsikkerhed eller under en sikkerhedssamtale

f) er blevet dømt for en eller flere straffelovsovertrædelser

g) har en fortid som alkoholiker eller bruger af ulovlig narkotika og/eller misbruger af lovlige stoffer

h) er eller har udvist en adfærd, der kan gøre den pågældende særlig sårbar over for pengeafpresning eller anden form for pres

i) gennem handling eller tale har udvist uærlighed, illoyalitet, upålidelighed eller utroværdighed

j) i alvorlig grad eller gentagne gange har overtrådt sikkerhedsregler eller har forsøgt at udføre eller har udført uautoriserede handlinger i forbindelse med kommunikations- og informationssystemer

k) kan risikere at blive udsat for pres (f.eks. i kraft af at være statsborger i et eller flere lande uden for EU eller i kraft af slægtninge eller nære forbindelser, der kan være sårbare over for påvirkning fra fremmede efterretningstjenester, terrorgrupper eller andre undergravende organisationer eller personer, hvis mål kan true EU's og/eller medlemsstaters sikkerhedsinteresser).

9. Når det er hensigtsmæssigt og i overensstemmelse med nationale love og bestemmelser, kan en persons økonomiske og medicinske baggrund også anses for at være relevant i forbindelse med sikkerhedsgodkendelsen.

10. Når det er hensigtsmæssigt og i overensstemmelse med nationale love og bestemmelser, kan en ægtefælles eller samlevers eller et nært familiemedlems karakter, adfærd eller situation ligeledes anses for at være relevant i forbindelse med sikkerhedsgodkendelsen.

Undersøgelseskrav med henblik på adgang til EUCI

Første tildeling af en PSC

11. Den første PSC med henblik på adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, baseres på en sikkerhedsundersøgelse, der går mindst fem år tilbage, eller som dækker perioden fra personens fyldte 18 år frem til nutiden, alt efter hvad der er kortest, og omfatter følgende:

a) udfyldelse af et nationalt spørgeskema om personelsikkerhed vedrørende den klassifikationsgrad for EUCI, som den pågældende kan få adgang til; når dette spørgeskema er udfyldt, sendes det til den kompetente sikkerhedsmyndighed

b) kontrol af identitet/statsborgerskab/nationalitet — personens fødselsdato, fødested og identitet kontrolleres. Personens statsborgerskab og/eller nationalitet, både nuværende og tidligere, fastslås; dette omfatter en vurdering af enhver sårbarhed over for pres fra udenlandsk side, f.eks. som følge af tidligere bopælsland eller tidligere tilhørsforhold, og

c) kontrol af nationale og lokale registre — oplysninger fra de nationale sikkerhedsregistre og centrale strafferegistre, hvor sådanne findes, og/eller andre tilsvarende statslige og politimæssige registre kontrolleres. Registre hos de retshåndhævende myndigheder med retlig kompetence på det sted, hvor personen har haft bopæl eller har været ansat, skal ligeledes kontrolleres.

12. Den første PSC med henblik på adgang til informationer, der er klassificeret TRES SECRET UE/EU TOP SECRET, baseres på en sikkerhedsundersøgelse, der går mindst ti år tilbage, eller som dækker perioden fra 18 år frem til nutiden, alt efter hvad der er kortest. Hvis der gennemføres samtaler som omhandlet i litra e), skal undersøgelserne gå mindst syv år tilbage eller dække perioden fra 18 år frem til nutiden, alt efter hvad der er kortest. Ud over de kriterier, der er omhandlet i punkt 8 ovenfor, skal de herunder opstillede forhold undersøges, så vidt det er muligt i henhold til nationale love og bestemmelser, inden der tildeles en PSC til klassifikationsgraden TRES SECRET UE/EU TOP SECRET; de kan også undersøges, inden der tildeles en PSC til klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, hvor det er påkrævet i henhold til nationale love og bestemmelser:

a) økonomisk status — der skal indhentes oplysninger om personens økonomiske forhold for at vurdere, om den pågældende på grund af alvorlige økonomiske vanskeligheder kan være sårbar over for udenlandsk eller indenlandsk pres, eller om den pågældende er påfaldende velstående

b) uddannelse — der skal indhentes oplysninger for at kontrollere personens uddannelsesmæssige baggrund på skoler, universiteter eller andre uddannelsesinstitutioner, hvor den pågældende har gået fra det fyldte 18. år eller i en periode, som den myndighed, der foretager undersøgelsen, finder relevant

c) beskæftigelse — der skal indhentes oplysninger om nuværende og tidligere beskæftigelse med henvisning til kilder såsom beskæftigelsesregistre, udtalelser om dygtighed eller effektivitet samt til arbejdsgivere eller overordnede

d) militærtjeneste — hvor det er relevant, kontrolleres en persons tjeneste i de væbnede styrker og fratrædelsesårsag, og

e) samtale — hvis der er hjemmel herfor i national lovgivning, skal der gennemføres en eller flere samtaler med den pågældende. Der gennemføres også samtaler med andre personer, som er i stand til at give en objektiv vurdering af den pågældendes baggrund, aktiviteter, loyalitet, troværdighed og pålidelighed. Hvis det er almindelig praksis i et land at anmode den person, som er genstand for undersøgelsen, om referencer, skal der afholdes en samtale med referencepersonerne, medmindre der er gode grunde til ikke at gøre det.

13. Når det er nødvendigt og i overensstemmelse med nationale love og bestemmelser, kan der gennemføres yderligere undersøgelser for at finde frem til alle relevante oplysninger om en person og for at bekræfte eller afkræfte negative oplysninger.

Fornyelse af en PSC

14. Har personen været i uafbrudt tjeneste i en national administration eller i GSR efter den første tildeling af en PSC, og har den pågældende fortsat behov for adgang til EUCI, skal PSC'en tages op til revision med henblik på fornyelse mindst hvert femte år for en sikkerhedsgodkendelse til klassifikationsgraden TRES SECRET UE/EU TOP SECRET og mindst hvert tiende år for en sikkerhedsgodkendelse til klassifikationsgraden SECRET UE/EU SECRET og CONFIDENTIEL UE/EU CONFIDENTIAL regnet fra datoen for meddelelsen af resultatet af den seneste sikkerhedsundersøgelse, som PSC'en er baseret på. Alle sikkerhedsundersøgelser med henblik på fornyelse af en PSC skal omfatte den periode, som er forløbet siden den foregående undersøgelse.

15. I forbindelse med fornyelsen af PSC'er skal de forhold, der er skitseret i punkt 11 og 12, undersøges.

16. Anmodninger om fornyelse skal indgives rettidigt under hensyntagen til den tid, der er nødvendig til sikkerhedsundersøgelser. Såfremt den relevante NSA eller anden kompetent national myndighed har modtaget den relevante anmodning om fornyelse og det tilsvarende spørgeskema om personelsikkerhed, inden en PSC udløber, og den nødvendige sikkerhedsundersøgelse ikke er afsluttet, kan den kompetente nationale myndighed, hvis der er hjemmel herfor i nationale love og bestemmelser, dog forlænge gyldigheden af den eksisterende PSC i en periode på op til 12 måneder. Hvis sikkerhedsundersøgelsen stadig ikke er afsluttet ved udløbet af denne periode på 12 måneder, skal den pågældende person pålægges arbejdsopgaver, der ikke kræver en PSC.

PSC-procedurer i GSR

17. For tjenestemænd og øvrige ansatte i GSR fremsender GSR's sikkerhedsmyndighed det udfyldte spørgeskema om personelsikkerhed til NSA'en i den medlemsstat, hvor den pågældende er statsborger, og anmoder om, at der foretages en sikkerhedsundersøgelse med henblik på den klassifikationsgrad for EUCI, som den pågældende skal have adgang til.

18. Hvis GSR får kendskab til oplysninger, der er relevante for en sikkerhedsundersøgelse, om en person, der har ansøgt om en EU-PSC, underretter GSR den relevante NSA herom i overensstemmelse med de relevante regler og bestemmelser.

19. Efter gennemførelsen af sikkerhedsundersøgelsen underretter den relevante NSA GSR's sikkerhedsmyndighed om resultatet af undersøgelsen under anvendelse af det standardformat for korrespondance, der er foreskrevet af Sikkerhedsudvalget.

a) Hvis sikkerhedsundersøgelsen fører til den konklusion, at der ikke er konstateret negative forhold, som kan rejse tvivl om personens loyalitet, troværdighed og pålidelighed, kan GSR's ansættelsesmyndighed tildele den pågældende en EU-PSC og tillade adgang til EUCI op til den relevante klassifikationsgrad indtil en bestemt dato.

b) Hvis sikkerhedsundersøgelsen ikke fører til denne konklusion, underretter GSR's ansættelsesmyndighed den pågældende person, der kan anmode om at blive hørt af ansættelsesmyndigheden. Ansættelsesmyndigheden kan anmode den kompetente NSA om de nærmere oplysninger, som denne er i stand til at give i henhold til de nationale love og bestemmelser. Såfremt resultatet bekræftes, kan der ikke tildeles en EU-PSC.

20. Sikkerhedsundersøgelsen samt de opnåede resultater er underlagt de relevante love og bestemmelser, som er gældende i den pågældende medlemsstat, herunder bestemmelser om klageadgang. Der kan indgives klager over afgørelser truffet af GSR's ansættelsesmyndighed i overensstemmelse med vedtægten for tjenestemænd ved Den Europæiske Union og ansættelsesvilkårene for de øvrige ansatte ved Den Europæiske Union, som fastsat i forordning (EØF, Euratom, EKSF) nr. 259/68 [1] (i det følgende benævnt »personalevedtægten og ansættelsesvilkårene«).

21. Den sikkerhedskonklusion, som en EU-PSC er baseret på, forudsat at den stadig er gyldig, omfatter alle de arbejdsopgaver, den pågældende person udfører inden for GSR eller Kommissionen.

22. Hvis en persons ansættelsesperiode ikke påbegyndes inden for 12 måneder efter meddelelsen af sikkerhedsundersøgelsens resultat til GSR's ansættelsesmyndighed, eller hvis personens ansættelse afbrydes i en periode på 12 måneder, uden at der i samme periode sker ansættelse i GSR eller i en medlemsstats nationale forvaltning, skal dette resultat meddeles den relevante NSA med henblik på at få bekræftet, at det fortsat er gyldigt og relevant.

23. Hvis GSR får kendskab til oplysninger om, at en person, der er i besiddelse af en gyldig EU-PSC, udgør en sikkerhedsrisiko, underretter GSR den relevante NSA herom i overensstemmelse med de relevante regler og bestemmelser. Når en NSA underretter GSR om, at den trækker en sikkerhedskonklusion tilbage, der er givet i overensstemmelse med punkt 19, litra a), vedrørende en person, der er i besiddelse af en gyldig EU-PSC, kan GSR's ansættelsesmyndighed anmode NSA'en om de nærmere oplysninger, som denne er i stand til at give i henhold til de nationale love og bestemmelser. Hvis de negative oplysninger bekræftes, inddrages EU-PSC'en, og personen har ikke længere adgang til EUCI eller til stillinger, hvor en sådan adgang er mulig, eller hvor den pågældende ville kunne udgøre en sikkerhedsrisiko.

24. En beslutning om inddragelse af en EU-PSC fra en tjenestemand eller øvrig ansat ved GSR og, når det er relevant, grundene hertil meddeles den pågældende person, som kan anmode om at blive hørt af ansættelsesmyndigheden. Oplysninger, der videregives af en NSA, er underlagt de relevante love og bestemmelser, som er gældende i den pågældende medlemsstat, herunder bestemmelser om klageadgang. Der kan indgives klager over afgørelser truffet af GSR's ansættelsesmyndighed i overensstemmelse med personalevedtægten og ansættelsesvilkårene.

25. Nationale eksperter, der udstationeres ved GSR i en stilling, hvortil der kræves en EU-PSC, skal fremlægge en gyldig national PSC for adgang til EUCI for GSR's sikkerhedsmyndighed, inden de påbegynder arbejdet.

Registre over PSC'er

26. Hver medlemsstat og GSR fører registre henholdsvis over de nationale PSC'er og EU-PSC'er, der er tildelt personer med henblik på adgang til EUCI. Disse registre skal mindst indeholde den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), datoen for tildelingen af PSC'en samt dens gyldighedsperiode.

27. Den kompetente sikkerhedsmyndighed kan udstede et certifikat for personelsikkerhedsgodkendelse (PSCC) med angivelse af den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), gyldighedsdatoen for den relevante nationale PSC for adgang til EUCI eller EU-PSC og certifikatets udløbsdato.

Undtagelser fra kravet om PSC

28. For personer i medlemsstaterne, der er behørigt autoriseret i kraft af deres funktioner, afgøres adgang til EUCI i overensstemmelse med nationale love og bestemmelser; disse personer skal gøres bekendt med deres sikkerhedsmæssige forpligtelser med hensyn til beskyttelse af EUCI.

IV. UDDANNELSE I OG BEVIDSTGØRELSE OM SIKKERHED

29. Alle personer, der har fået tildelt en PSC, skal skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og de konsekvenser, det kan få, hvis EUCI kompromitteres. Sådanne skriftlige bekræftelser registreres af medlemsstaten og GSR, afhængigt af hvad der er hensigtsmæssigt.

30. Alle personer, der er autoriseret til at have adgang til eller skal håndtere EUCI, skal indledningsvis gøres opmærksom på og med regelmæssige mellemrum gøres bekendt med sikkerhedsrisici og skal øjeblikkelig indberette enhver henvendelse eller aktivitet, de finder mistænkelig eller usædvanlig, til de relevante sikkerhedsmyndigheder.

31. Alle personer, der ikke længere udfører funktioner, der kræver adgang til EUCI, skal underrettes om og, når det er relevant, skriftligt bekræfte deres forpligtelser med hensyn til fortsat beskyttelse af EUCI.

[1] EFT L 56 af 4.3.1968, s. 1.

V. EKSTRAORDINÆRE OMSTÆNDIGHEDER

32. Hvis der er hjemmel herfor i nationale love og bestemmelser, kan en personelsikkerhedsgodkendelse, der er tildelt af en medlemsstats kompetente nationale myndighed med henblik på adgang til nationale klassificerede informationer, i en midlertidig periode, inden der tildeles en national PSC med henblik på adgang til EUCI, give nationale tjenestemænd adgang til EUCI op til en tilsvarende klassifikationsgrad, jf. den sammenlignende oversigt i tillæg B, hvis en sådan midlertidig adgang er påkrævet af hensyn til EU's interesser. NSA'erne underretter Sikkerhedsudvalget, hvis nationale love og bestemmelser ikke tillader en sådan midlertidig adgang til EUCI.

33. GSR's ansættelsesmyndighed kan i hastetilfælde, hvor det er behørigt begrundet i tjenestens interesse, og inden en fuldstændig sikkerhedsundersøgelse er afsluttet, efter samråd med NSA'en i den medlemsstat, hvor den pågældende er statsborger, og med forbehold af resultatet af en foreløbig kontrol for at undersøge, at der ikke er konstateret negative oplysninger, give tjenestemænd og øvrige ansatte ved GSR midlertidig autorisation til at få adgang til EUCI med henblik på en specifik opgave. Sådanne midlertidige autorisationer er gyldige i en periode, der ikke overstiger seks måneder, og tillader ikke adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET. Alle personer, der har fået en midlertidig autorisation, skal skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og konsekvenserne af en eventuel kompromittering af EUCI. GSR fører et register over sådanne skriftlige bekræftelser.

34. Når en person skal tiltræde en stilling, hvortil der kræves en PSC med en højere klassifikationsgrad end den, den pågældende allerede har, kan tiltrædelsen ske midlertidigt, forudsat at:

a) den pågældendes foresatte skriftligt dokumenterer, at der er et tvingende behov for adgang til EUCI af en højere klassifikationsgrad

b) adgangen er begrænset til bestemte EUCI til brug for arbejdsopgaverne

c) den pågældende er i besiddelse af en gyldig national PSC eller EU-PSC

d) der er iværksat foranstaltninger til at opnå autorisation til den klassifikationsgrad, som er påkrævet til stillingen

e) den kompetente myndighed i tilstrækkeligt omfang har kontrolleret, at den pågældende ikke har begået alvorlige eller gentagne overtrædelser af sikkerhedsreglerne

f) den pågældendes varetagelse af arbejdsopgaverne godkendes af den kompetente myndighed, og

g) undtagelsen registreres i den ansvarlige registratur eller underregistratur med en beskrivelse af de informationer, der er givet adgang til.

35. Ovennævnte procedure anvendes for engangsadgang til EUCI med en klassifikationsgrad, der er ét trin højere end den, personen er sikkerhedsgodkendt til. Der må ikke gøres tilbagevendende brug af denne procedure.

36. Under ganske særlige omstændigheder, f.eks. i forbindelse med missioner i fjendtlige miljøer eller under en eskalerende international krise, kan medlemsstaterne og generalsekretæren, såfremt det er tvingende nødvendigt, især for at redde menneskeliv, give tilladelse, så vidt muligt skriftligt, til, at personer, der ikke har den krævede PSC, får adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, hvis en sådan tilladelse er absolut nødvendig, og der ikke er rimelige grunde til at betvivle de pågældende personers loyalitet, troværdighed og pålidelighed. Denne tilladelse skal registreres med en beskrivelse af de informationer, der er givet adgang til.

37. Drejer det sig om informationer, der er klassificeret TRES SECRET UE/EU TOP SECRET, begrænses denne nødadgang til EU-borgere, som allerede er autoriseret til at have adgang enten til den nationale klassifikationsgrad, der svarer til TRES SECRET UE/EU TOP SECRET, eller til informationer, der er klassificeret SECRET UE/EU SECRET.

38. Sikkerhedsudvalget underrettes om tilfælde, hvor proceduren i punkt 36 og 37 anvendes.

39. Hvis en medlemsstats nationale love og bestemmelser fastsætter strengere regler for personers adgang til klassificerede informationer i forbindelse med midlertidige autorisationer, midlertidige arbejdsopgaver, engangsadgang eller nødadgang, gennemføres procedurerne i dette afsnit kun inden for de begrænsninger, der er fastsat i de relevante nationale love og bestemmelser.

40. Sikkerhedsudvalget forelægges hvert år en rapport om anvendelsen af procedurerne i dette afsnit.

VI. DELTAGELSE I MØDER I RÅDET

41. Når personer skal deltage i møder i Rådet eller Rådets forberedende organer, hvor der drøftes informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal deres PSC-status bekræftes, jf. dog punkt 28. For delegerede fremsendes et PSCC eller anden dokumentation for PSC af de relevante myndigheder til GSR's Sikkerhedskontor, eller de forelægges undtagelsesvis af den pågældende delegerede. Der kan eventuelt anvendes en konsolideret navneliste, som indeholder den relevante dokumentation for PSC.

42. Hvis en national PSC for adgang til EUCI af sikkerhedsgrunde inddrages fra en person, hvis arbejdsopgaver kræver deltagelse i møder i Rådet eller Rådets forberedende organer, underretter den kompetente myndighed GSR herom.

VII. POTENTIEL ADGANG TIL EUCI

43. Når personer skal ansættes under forhold, hvor de eventuelt kan få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal de sikkerhedsgodkendes på behørig vis eller skal til stadighed ledsages.

44. Kurerer, vagter og eskorter skal sikkerhedsgodkendes til den relevante klassifikationsgrad eller på anden vis undersøges i passende omfang i overensstemmelse med nationale love og bestemmelser, gøres bekendt med sikkerhedsprocedurer til beskyttelse af EUCI og orienteres om de forpligtelser, der påhviler dem med hensyn til beskyttelse af de informationer, de får betroet.

BILAG II

FYSISK SIKKERHED

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 8. Det fastsætter mindstekrav til den fysiske beskyttelse af lokaliteter, bygninger, kontorer, lokaler og andre områder, hvor EUCI håndteres og opbevares, herunder områder, der huser CIS'er.

2. De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre uautoriseret adgang til EUCI ved:

   a) at sikre, at EUCI håndteres og opbevares hensigtsmæssigt

   b) at muliggøre personalemæssig adskillelse for så vidt angår adgang til EUCI på grundlag af personalets need-to-know og, når det er relevant, dets sikkerhedsgodkendelse

   c) at afskrække fra, vanskeliggøre og afsløre uautoriserede handlinger og

   d) at forhindre eller forsinke, at indtrængere skaffer sig hemmelig adgang eller tiltvinger sig adgang.

II. FYSISKE SIKKERHEDSKRAV OG -FORANSTALTNINGER

3. De fysiske sikkerhedsforanstaltninger udvælges på grundlag af de kompetente myndigheders trusselsvurdering. GSR og medlemsstaterne skal anvende en risikostyringsproces med henblik på sikkerhedsbeskyttelse af EUCI i deres lokaliteter for at sikre, at der anvendes et fysisk beskyttelsesniveau, der svarer til den vurderede risiko. Risikostyringsprocessen skal tage hensyn til alle relevante faktorer, navnlig:

   a) EUCI's klassifikationsgrad

   b) formen og mængden af EUCI under hensyn til, at store mængder eller en samling af EUCI kan kræve, at der skal anvendes strengere beskyttelsesforanstaltninger

   c) omgivelserne og strukturen af de bygninger eller områder, hvor EUCI opbevares, og

   d) den vurderede trussel fra efterretningstjenester, der har EU eller medlemsstaterne som mål, samt fra sabotage, terrorisme og undergravende eller anden kriminel virksomhed.

4. Den kompetente sikkerhedsmyndighed fastlægger under anvendelse af begrebet dybdeforsvar den rette kombination af de fysiske sikkerhedsforanstaltninger, der skal iværksættes. De kan omfatte en eller flere af følgende foranstaltninger:

   a) en perimeterafspærring: en fysisk afspærring, der afgrænser et område, som kræver sikkerhedsbeskyttelse

   b) system til afsløring af indtrængen (IDS): et IDS kan anvendes for at øge det sikkerhedsniveau, en perimeterafspærring giver, eller anvendes i rum og bygninger i stedet for sikkerhedspersonale eller for at bistå dette personale

   c) adgangskontrol: der kan foretages adgangskontrol ved et anlæg, en bygning eller flere bygninger i et anlæg eller i forbindelse med områder eller rum inde i en bygning. Kontrollen kan foretages elektronisk, elektromekanisk, udføres af sikkerhedspersonale og/eller en receptionist eller ved hjælp af andre fysiske metoder

   d) sikkerhedspersonale: der kan ansættes sikkerhedspersonale, der er uddannet, er under tilsyn og, når det er nødvendigt, har en relevant sikkerhedsgodkendelse bl.a. for at afskrække personer, der planlægger hemmelig indtrængen

   e) intern tv-overvågning (CCTV): sikkerhedspersonalet kan anvende CCTV for at kontrollere hændelser og IDS-alarmer på store anlæg eller langs perimetre

   f) sikkerhedsbelysning: der kan anvendes sikkerhedsbelysning for at afskrække en potentiel indtrænger og for at skaffe den belysning, der er nødvendig for en effektiv overvågning foretaget direkte af sikkerhedspersonalet eller indirekte ved hjælp af et CCTV-system, og

   g) eventuelle andre passende fysiske foranstaltninger, der skal afskrække fra eller afsløre uautoriseret adgang eller forhindre tab af eller skade på EUCI.

5. Den kompetente myndighed kan bemyndiges til at foretage visitation ved ind- og udgang som afskrækkelse mod uautoriseret indførelse af materiale eller uautoriseret fjernelse af EUCI fra lokaliteter eller bygninger.

6. Når der er risiko for indblik i EUCI, selv uforsætligt, skal der træffes passende foranstaltninger til at imødegå denne risiko.

7. I forbindelse med nye faciliteter skal der defineres fysiske sikkerhedskrav og funktionelle specifikationer som en del af planlægningen og udformningen af faciliteterne. I forbindelse med eksisterende faciliteter skal de fysiske sikkerhedskrav opfyldes i videst mulig udstrækning.

III. UDSTYR TIL FYSISK BESKYTTELSE AF EUCI

8. Når der skal anskaffes udstyr (f.eks. sikkerhedscontainere, makulatorer, dørlåse, elektroniske adgangskontrolsystemer, IDS, alarmsystemer) til fysisk beskyttelse af EUCI, skal den kompetente sikkerhedsmyndighed sikre, at udstyret opfylder de godkendte tekniske standarder og minimumskrav.

9. De tekniske specifikationer for udstyr, der skal anvendes til fysisk beskyttelse af EUCI, fastsættes i sikkerhedsretningslinjer, der skal godkendes af Sikkerhedsudvalget.

10. Sikkerhedssystemer skal inspiceres med jævne mellemrum, og udstyret skal vedligeholdes regelmæssigt. Vedligeholdelsesarbejdet skal tage hensyn til resultatet af inspektionerne for at sikre, at udstyret fortsat fungerer optimalt.

11. Effektiviteten af de individuelle sikkerhedsforanstaltninger og af det samlede sikkerhedssystem skal reevalueres ved hver inspektion.

IV. FYSISK BESKYTTEDE OMRÅDER

12. Der etableres to typer fysisk beskyttede områder, eller nationale pendanter hertil, med henblik på den fysiske beskyttelse af EUCI:

    a) administrative områder og

    b) sikrede områder (herunder teknisk sikrede områder).

    I denne afgørelse omfatter enhver omtale af administrative områder og sikrede områder, herunder teknisk sikrede områder, også nationale pendanter hertil.

13. Den kompetente sikkerhedsmyndighed bestemmer, at et område opfylder kravene til at blive betegnet som et administrativt område, et sikret område eller et teknisk sikret område.

14. For så vidt angår administrative områder:

    a) der etableres en synligt afgrænset perimeter, der muliggør kontrol af personer og, når det er muligt, af køretøjer

    b) uledsaget adgang tillades kun for personer, der er behørigt autoriseret af den kompetente myndighed, og

    c) alle andre personer skal til stadighed ledsages eller underkastes tilsvarende kontrol.

15. For så vidt angår sikrede områder:

    a) der etableres en synligt afgrænset og beskyttet perimeter, hvor al ind- og udgang kontrolleres ved hjælp af et adgangskort eller et persongenkendelsessystem

    b) uledsaget adgang tillades kun for personer, der er sikkerhedsgodkendt og specifikt bemyndiget til at komme ind på området på grundlag af deres need-to-know

    c) alle andre personer skal til stadighed ledsages eller underkastes tilsvarende kontrol.

16. Hvis adgang til et sikret område i praksis indebærer direkte adgang til de klassificerede informationer, der opbevares deri, gælder følgende yderligere krav:

    a) den højeste sikkerhedsklassifikationsgrad for de informationer, der normalt opbevares i området, skal klart angives

    b) alle besøgende skal have en specifik autorisation til at få adgang til området, skal til stadighed ledsages og skal være passende sikkerhedsgodkendt, medmindre der træffes foranstaltninger, der sikrer, at der ikke er mulighed for adgang til EUCI.

17. Sikrede områder, der er beskyttet mod aflytning, udpeges som teknisk sikrede områder. Følgende yderligere krav gælder:

    a) sådanne områder skal udstyres med IDS, være aflåst, når de ikke er i brug, og være bevogtet, når de er i brug. Eventuelle nøgler skal kontrolleres i overensstemmelse med afsnit VI

    b) alle personer og alt materiel, der kommer ind i disse områder, skal kontrolleres

    c) områderne skal underkastes regelmæssige fysiske og/eller tekniske inspektioner som krævet af den kompetente sikkerhedsmyndighed. Inspektionerne skal desuden foretages efter en eventuel uautoriseret adgang eller ved mistanke om, at en sådan adgang har fundet sted, og

    d) områderne må ikke indeholde uautoriserede kommunikationslinjer, uautoriserede telefoner eller andre uautoriserede kommunikationsanordninger og uautoriseret elektrisk eller elektronisk udstyr.

18. Inden der skal anvendes kommunikationsanordninger og elektrisk eller elektronisk udstyr af enhver art i områder, hvor der afholdes møder om eller arbejdes med informationer, der er klassificeret SECRET UE/EU SECRET eller højere, og når truslen for EUCI vurderes som værende stor, skal dette udstyr uanset punkt 17, litra d), først undersøges af den kompetente sikkerhedsmyndighed for at sikre, at ingen forståelige informationer uagtsomt eller ulovligt transmitteres ud af det sikrede områdes perimeter ved hjælp af sådant udstyr.

19. Sikrede områder, hvor der ikke er vagtpersonale døgnet rundt, skal, når det er relevant, inspiceres ved afslutningen af normal arbejdstid og med tilfældige intervaller uden for normal arbejdstid, medmindre der findes et IDS.

20. Sikrede områder og teknisk sikrede områder kan etableres midlertidigt inden for et administrativt område med henblik på at afholde et klassificeret møde eller til et andet lignende formål.

21. Der skal udarbejdes operationelle sikkerhedsprocedurer for hvert sikret område, der indeholder bestemmelser om:

    a) klassifikationsgraden for de EUCI, der kan håndteres og opbevares i området

    b) de overvågnings- og beskyttelsesforanstaltninger, der skal opretholdes

    c) de personer, der er autoriseret til at have uledsaget adgang til området i kraft af deres need-to-know og sikkerhedsgodkendelse

    d) når det er relevant, procedurerne for ledsagelse eller for sikkerhedsbeskyttelse af EUCI, når andre personer autoriseres til at få adgang til området

    e) andre relevante foranstaltninger og procedurer.

22. Der skal bygges bokslokaler inden for sikrede områder. Vægge, gulve, lofter, vinduer og låsbare døre skal godkendes af den kompetente sikkerhedsmyndighed og yde tilsvarende beskyttelse som den, en sikkerhedscontainer, der er godkendt til opbevaring af EUCI af samme klassifikationsgrad, yder.

V. FYSISKE BESKYTTELSESFORANSTALTNINGER MED HENBLIK PÅ HÅNDTERING OG OPBEVARING AF EUCI

23. EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, kan håndteres:

    a) i et sikret område

    b) i et administrativt område, forudsat at EUCI er beskyttet mod uautoriserede personers adgang, eller

    c) uden for et sikret område eller et administrativt område, forudsat at den, der er i besiddelse af informationerne, transporterer EUCI i overensstemmelse med bilag III, punkt 28-40 og har lovet at overholde kompenserende foranstaltninger, der er fastlagt i sikkerhedsinstruktioner udstedt af den kompetente sikkerhedsmyndighed, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang.

24. EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, skal opbevares i passende aflåste kontormøbler i et administrativt område eller et sikret område. De kan opbevares midlertidigt uden for et sikret område eller et administrativt område forudsat at den, der er i besiddelse af informationerne, har lovet at overholde kompenserende foranstaltninger, der er fastlagt i sikkerhedsinstruktioner udstedt af den kompetente sikkerhedsmyndighed.

25. EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, kan håndteres:

a) i et sikret område

b) i et administrativt område, forudsat at EUCI er beskyttet mod uautoriserede personers adgang, eller

c) uden for et sikret område eller et administrativt område, forudsat at den, der er i besiddelse af informationerne:

i) transporterer EUCI i overensstemmelse med bilag III, punkt 28-40

ii) har lovet at overholde kompenserende foranstaltninger, der er fastlagt i sikkerhedsinstruktioner udstedt af den kompetente sikkerhedsmyndighed, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang

iii) til enhver tid har EUCI under personlig kontrol og

iv) i tilfælde af dokumenter i papirform har underrettet den relevante registratur om situationen.

26. EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, skal opbevares i et sikret område i en sikkerhedscontainer eller et bokslokale.

27. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal håndteres i et sikret område.

28. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal opbevares i et sikret område under et af følgende forhold:

a) i en sikkerhedscontainer, jf. punkt 8, med en eller flere af følgende former for supplerende kontrol:

i) permanent beskyttelse eller kontrol foretaget af sikkerhedsgodkendt sikkerhedspersonale eller vagtpersonale

ii) et godkendt IDS kombineret med indsatssikkerhedspersonale

eller

b) i et bokslokale udstyret med IDS og kombineret med indsatssikkerhedspersonale.

29. Regler for transport af EUCI uden for fysisk beskyttede områder findes i bilag III.

VI. KONTROL MED NØGLER OG KODER, DER ANVENDES TIL SIKKERHEDSBESKYTTELSE AF EUCI

30. Den kompetente sikkerhedsmyndighed fastsætter procedurer for forvaltning af nøgler og koder til kontorer, rum, bokslokaler og sikkerhedscontainere. Sådanne procedurer skal beskytte mod uautoriseret adgang.

31. Koder skal læres udenad af det mindst mulige antal personer, der har behov for at kende dem. Koder til sikkerhedscontainere og bokslokaler, hvor der opbevares EUCI, skal ændres:

a) når der sker en ændring i det personale, der kender koden

b) når der er konstateret en kompromittering, eller der er mistanke herom

c) når der er foretaget vedligeholdelse eller reparation af en lås, og

d) mindst hver 12. måned.

BILAG III

FORVALTNING AF KLASSIFICEREDE INFORMATIONER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 9. Det fastsætter de administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus for at bidrage til at afskrække fra, afsløre og udbedre skade forårsaget af forsætlig eller uagtsom kompromittering eller tab af sådanne informationer.

II. KLASSIFIKATIONSSTYRING

Klassifikation og mærkning

2. Informationer klassificeres, hvis de kræver beskyttelse med hensyn til fortroligheden.

3. Det er udstederen af EUCI, der er ansvarlig for at fastlægge klassifikationsgraden i overensstemmelse med de relevante klassifikationsretningslinjer og for den første udbredelse af informationerne.

4. EUCI's klassifikationsgrad fastlægges i overensstemmelse med artikel 2, stk. 2, og ved henvisning til den sikkerhedspolitik, der godkendes i henhold til artikel 3, stk. 3.

5. Sikkerhedsklassifikationen skal fremgå klart og korrekt, uanset om EUCI gives i papirform, mundtligt, elektronisk eller i en anden form.

6. De enkelte dele af et dokument (dvs. sider, afsnit og punkter i et dokument samt bilag, tillæg og vedhæftet materiale) kan kræve forskellig klassifikationsgrad, og skal mærkes i overensstemmelse hermed, også under opbevaring i elektronisk form.

7. Et dokuments eller dossiers samlede klassifikationsgrad skal mindst være den samme som den del, der har den højeste klassifikationsgrad. Når informationer er indsamlet fra forskellige kilder, skal det endelige produkt tages op til revision for at fastlægge dets samlede klassifikationsgrad, da det kan tilsige en højere klassifikationsgrad end de enkelte dele.

8. I videst muligt omfang skal dokumenter, der indeholder dele med forskellig klassifikationsgrad, struktureres, så dele med en anden klassifikationsgrad let kan identificeres og udskilles, hvis det er nødvendigt.

9. En følgeskrivelse klassificeres lige så højt som bilagenes højeste klassifikationsgrad. Udstederen skal klart ved hjælp af en passende mærkning angive, på hvilket niveau følgeskrivelsen skal klassificeres, hvis den adskilles fra sine bilag, f.eks.

CONFIDENTIEL UE/EU CONFIDENTIAL

Uden vedhæftet materiale RESTREINT UE/EU RESTRICTED

Mærkning

10. Ud over en af de klassifikationsmærkninger, der er nævnt i artikel 2, stk. 2, kan EUCI forsynes med yderligere mærkninger, f.eks. med:

a) en identifikator for at angive udstederen

b) eventuelle særlige påtegninger, kodeord eller akronymer, der angiver det aktivitetsområde, som dokumentet omhandler, en særlig distribution på need-to-know-basis eller begrænset anvendelse

c) påtegning om mulighederne for videregivelse

d) eventuelt den dato eller den specifikke begivenhed, efter hvilken de kan nedklassificeres eller afklassificeres.

Forkortede klassifikationsmærkninger

11. Standardiserede forkortede klassifikationsmærkninger kan anvendes for at angive klassifikationsgraden for de enkelte afsnit af en tekst. Forkortelserne erstatter ikke den uforkortede klassifikationsmærkning.

12. Følgende standardforkortelser kan anvendes i EU's klassificerede dokumenter for at angive afsnits eller tekstdeles klassifikationsgrad, hvis teksten er kortere end en enkelt side:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Udarbejdelse af EUCI

13. Når der udarbejdes et klassificeret EU-dokument,

a) skal hver side være tydeligt mærket med klassifikationsgraden

b) skal hver side nummereres

c) skal dokumentet være forsynet med et referencenummer og et emne, der ikke i sig selv er en klassificeret information, medmindre det er mærket som sådan

d) skal dokumentet være forsynet med dato

e) skal dokumenter, der er klassificeret SECRET UE/EU SECRET eller højere, have et eksemplarnummer på hver side, hvis de skal udsendes i flere eksemplarer.

14. Hvis punkt 13 ikke kan finde anvendelse på EUCI, træffes der andre passende foranstaltninger i overensstemmelse med de sikkerhedsretningslinjer, der skal fastlægges i medfør af artikel 6, stk. 2.

Nedklassificering og afklassificering af EUCI

15. På det tidspunkt, hvor informationerne udarbejdes, angiver udstederen så vidt muligt og især i forbindelse med informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, om EUCI kan nedklassificeres eller afklassificeres på en bestemt dato eller efter en specifik begivenhed.

16. GSR tager regelmæssigt EUCI i dets besiddelse op til revision for at vurdere, om klassifikationsgraden fortsat skal finde anvendelse. GSR opretter et system, således at klassifikationsgraden af registrerede EUCI, som det har udfærdiget, tages op til revision mindst hvert femte år. En sådan revision er ikke nødvendig, hvis udstederen fra begyndelsen har angivet, at informationerne automatisk nedklassificeres eller afklassificeres, og informationerne er mærket i overensstemmelse hermed.

III. SIKKERHEDSREGISTRERING AF EUCI

17. For alle organisatoriske enheder i GSR og i medlemsstaternes nationale administrationer, som håndterer EUCI, udpeges en ansvarlig registratur for at sikre, at EUCI håndteres i overensstemmelse med denne afgørelse. Registraturerne oprettes som sikrede områder som defineret i bilag II.

18. I denne afgørelse forstås ved sikkerhedsregistrering (i det følgende benævnt »registrering«) anvendelse af procedurer, som registrerer materialets livscyklus, inklusive dets udbredelse og destruktion.

19. Alt materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal registreres i dertil oprettede registraturer, når det ankommer til eller forlader en organisatorisk enhed.

20. Den centrale registratur i GSR fører en fortegnelse over alle klassificerede informationer, der videregives af Rådet og GSR til tredjelande og internationale organisationer, og over alle klassificerede informationer, der modtages fra tredjelande eller internationale organisationer.

21. I forbindelse med et CIS kan registreringsprocedurerne gennemføres ved processer i selve CIS'et.

22. Rådet skal godkende en sikkerhedspolitik for sikkerhedsregistrering af EUCI.

TRÈS SECRET UE/EU TOP SECRET-registraturer

23. Der oprettes en registratur i medlemsstaterne og i GSR, der skal fungere som central myndighed for modtagelse og afsendelse af informationer, der er klassificeret TRES SECRET UE/EU TOP SECRET. Der kan i det nødvendige omfang oprettes underregistraturer, der håndterer disse informationer i registreringsøjemed.

24. Underregistraturer må ikke sende TRÈS SECRET UE/EU TOP SECRET-dokumenter direkte til andre underregistraturer under samme centrale TRÈS SECRET UE/EU TOP SECRET-registratur eller til anden side uden sidstnævntes udtrykkelige skriftlige godkendelse.

IV. KOPIERING OG OVERSÆTTELSE AF EU's KLASSIFICEREDE DOKUMENTER

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

26. Hvis udstederen af dokumenter, der er klassificeret SECRET UE/EU SECRET eller lavere, ikke har stillet særlige betingelser for kopiering eller oversættelse af dem, kan sådanne dokumenter kopieres eller oversættes efter instruks fra den, der er i besiddelse af dem.

27. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, gælder også for kopier og oversættelser af det.

V. TRANSPORT AF EUCI

28. Transport af EUCI er omfattet af beskyttelsesforanstaltningerne i punkt 30-40. Ved transport af EUCI ved hjælp af elektroniske medier kan nedennævnte sikkerhedsforanstaltninger uanset artikel 9, stk. 4, suppleres med de relevante tekniske modforanstaltninger som foreskrevet af den kompetente sikkerhedsmyndighed med henblik på at minimere risikoen for tab eller kompromittering.

29. De kompetente sikkerhedsmyndigheder i GSR og i medlemsstaterne udfærdiger instruktioner for transport af EUCI i overensstemmelse med denne afgørelse.

I en bygning eller en selvstændig gruppe af bygninger

30. EUCI, der transporteres i en bygning eller en selvstændig gruppe af bygninger, skal tildækkes for at forhindre observation af deres indhold.

31. I en bygning eller en selvstændig gruppe af bygninger skal informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, transporteres i en sikret kuvert, hvorpå kun modtagerens navn er angivet.

Inden for EU

32. EUCI, der transporteres mellem bygninger eller lokaliteter inden for EU, skal pakkes således, at de er beskyttet mod uautoriseret videregivelse.

33. Transport af informationer, der er klassificeret SECRET UE/EU SECRET eller lavere, skal ske på en af følgende måder:

a) militær, officiel eller diplomatisk kurer, alt efter hvad der er hensigtsmæssigt

b) håndbåret under forudsætning af:

i) at EUCI forbliver i bærerens besiddelse, medmindre de opbevares i overensstemmelse med kravene i bilag II

ii) at EUCI ikke åbnes undervejs eller læses på offentlige steder

iii) at enkeltpersoner gøres bekendt med deres sikkerhedsansvar

iv) at enkeltpersoner om nødvendigt får udstedt et kurercertifikat.

c) nationale posttjenester eller kommercielle kurertjenester under forudsætning af:

i) at de er godkendt af den relevante NSA i overensstemmelse med nationale love og bestemmelser

ii) at de anvender passende beskyttelsesforanstaltninger i overensstemmelse med de minimumskrav, der skal fastsættes i sikkerhedsretningslinjerne i medfør af artikel 6, stk. 2.

Ved transport fra en medlemsstat til en anden finder bestemmelserne i litra c) kun anvendelse på informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller lavere.

34. Materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET (f.eks. udstyr eller maskiner), der ikke kan transporteres på de i punkt 33 omhandlede måder, transporteres som fragt af kommercielle fragtfirmaer i overensstemmelse med bilag V.

35. Transport af informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, mellem bygninger eller lokaliteter inden for EU, skal ske ved hjælp af militær, officiel eller diplomatisk kurer, alt efter hvad der er hensigtsmæssigt.

Fra EU til et tredjelands område

36. EUCI, der transporteres fra EU til et tredjelands område, skal pakkes således, at de er beskyttet mod uautoriseret videregivelse.

37. Transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, fra EU til et tredjelands område, skal ske på en af følgende måder:

a) militær eller diplomatisk kurer

b) håndbåret under forudsætning af:

i) at pakken er plomberet med et officielt segl eller er pakket, så det fremgår, at det drejer sig om en officiel forsendelse, som ikke skal underkastes told- eller sikkerhedskontrol

ii) at enkeltpersoner er i besiddelse af et kurercertifikat, der identificerer pakken og autoriserer dem til at transportere den

iii) at EUCI forbliver i bærerens besiddelse, medmindre de opbevares i overensstemmelse med kravene i bilag II

iv) at EUCI ikke åbnes undervejs eller læses på offentlige steder, og

v) at enkeltpersoner gøres bekendt med deres sikkerhedsansvar.

38. Transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, og som videregives af EU til et tredjeland eller en international organisation, skal overholde de relevante bestemmelser i en informationssikkerhedsaftale eller en administrativ ordning i henhold til artikel 12, stk. 2, litra a) eller b).

39. Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, kan også transporteres af posttjenester eller kommercielle kurertjenester.

40. Transport af informationer, der er klassificeret SECRET UE/EU TOP SECRET, fra EU til et tredjelands område, skal ske ved hjælp af militær eller diplomatisk kurer.

VI. DESTRUKTION AF EUCI

41. EU's klassificerede dokumenter, som der ikke længere er brug for, kan destrueres, jf. dog de relevante regler og bestemmelser om arkivering.

42. Dokumenter, der er omfattet af registrering i henhold til artikel 9, stk. 2, destrueres af den ansvarlige registratur efter anvisning fra den, der er i besiddelse af dem, eller fra en kompetent myndighed. Journalerne og andre registreringsinformationer ajourføres i overensstemmelse hermed.

43. For så vidt angår dokumenter, der er klassificeret SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, foretages destruktionen i overværelse af et vidne, der er sikkerhedsgodkendt til mindst den klassifikationsgrad, som det destruerede dokument har.

44. Den registeransvarlige og vidnet, hvis dettes tilstedeværelse er påkrævet, underskriver en destruktionsattest, der opbevares i registraturen. Registraturen opbevarer destruktionsattester vedrørende dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, i en periode på mindst ti år og vedrørende dokumenter, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, i en periode på mindst fem år.

45. Klassificerede dokumenter, herunder dokumenter, der er klassificeret RESTREINT UE/EU RESTRICTED, destrueres ved metoder, som opfylder de relevante EU-standarder eller tilsvarende standarder eller er godkendt af medlemsstaterne i overensstemmelse med nationale tekniske standarder, for at forhindre hel eller delvis rekonstruktion.

46. Destruktion af edb-lagringsmedier, der anvendes til lagring af EUCI, foregår i overensstemmelse med bilag IV, punkt 36.

VII. INSPEKTIONER OG VURDERINGSBESØG

47. Ordet »inspektion« anvendes i det følgende som betegnelse for enhver form for

a) inspektion i henhold til artikel 9, stk. 3, og artikel 15, stk. 2, litra e), f) og g), eller

b) vurderingsbesøg i henhold til artikel 12, stk. 5,

for at evaluere effektiviteten af foranstaltninger til beskyttelse af EUCI.

48. Inspektioner udføres bl.a. for:

a) at sikre, at de krævede minimumstandarder for beskyttelse af EUCI, der er fastlagt i denne afgørelse, overholdes

b) at understrege betydningen af sikkerhed og effektiv risikostyring i de inspicerede enheder

c) at anbefale modforanstaltninger for at afbøde de specifikke virkninger i tilfælde af tab af klassificerede informationers fortrolighed, integritet eller tilgængelighed, og

d) at styrke sikkerhedsmyndighedernes løbende uddannelses- og bevidstgørelsesprogrammer vedrørende sikkerhed.

49. Inden udgangen af hvert kalenderår vedtager Rådet det inspektionsprogram, der er fastsat i artikel 15, stk. 1, litra c), for det efterfølgende år. De faktiske datoer for hver inspektion fastlægges efter aftale med det EU-agentur eller -organ, den medlemsstat, det tredjeland eller den internationale organisation, der er berørt.

Gennemførelse af inspektioner

50. Inspektioner gennemføres for at kontrollere den inspicerede enheds relevante regler, forskrifter og procedurer og for at kontrollere, at enhedens praksis er i overensstemmelse med grundprincipperne og minimumsstandarderne i denne afgørelse og i bestemmelserne for udveksling af klassificerede informationer med den pågældende enhed.

51. Inspektioner gennemføres i to faser. Forud for selve inspektionen tilrettelægges der om nødvendigt et forberedende møde med den pågældende enhed. Efter dette forberedende møde opstiller inspektionsholdet efter aftale med den pågældende enhed et detaljeret inspektionsprogram, der omfatter alle sikkerhedsområder. Inspektionsholdet skal have adgang til alle steder, hvor der håndteres EUCI, navnlig de steder, hvor registraturerne og CIS'erne findes.

52. Inspektioner i medlemsstaternes nationale administrationer gennemføres under ansvar af et fælles inspektionshold fra GSR og Kommissionen i fuldt samarbejde med medarbejdere i den enhed, der inspiceres.

53. Inspektioner i tredjelande og internationale organisationer gennemføres under ansvar af et fælles inspektionshold fra GSR og Kommissionen i fuldt samarbejde med medarbejdere i det tredjeland eller i den internationale organisation, der inspiceres.

54. Inspektioner af EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union samt af Europol og Eurojust gennemføres af GSR's Sikkerhedskontor med ekspertbistand fra den NSA, på hvis område agenturet eller organet er beliggende. Kommissionens Direktorat for Sikkerhed (ECSD) kan inddrages, i det omfang det regelmæssigt udveksler EUCI med det pågældende agentur eller organ.

55. Ved inspektioner af EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union samt af Europol og Eurojust og af tredjelande og internationale organisationer anmodes der om bistand og bidrag fra NSA-eksperter i overensstemmelse med detaljerede ordninger, der skal aftales med Sikkerhedsudvalget.

Inspektionsrapporter

56. Ved afslutningen af inspektionen forelægges de vigtigste konklusioner og anbefalinger for den inspicerede enhed. Der udarbejdes derefter en inspektionsrapport under GSR's sikkerhedsmyndigheds (Sikkerhedskontorets) ansvar. Hvis der foreslås korrigerende foranstaltninger og fremsættes anbefalinger, medtages der tilstrækkelige detaljer i rapporten til at understøtte konklusionerne. Inspektionsrapporten fremsendes til den relevante myndighed for den inspicerede enhed.

57. For så vidt angår inspektioner i medlemsstaternes nationale administrationer gælder følgende:

a) udkastet til inspektionsrapport fremsendes til vedkommende NSA for at kontrollere, at den er faktuelt korrekt, og at den ikke indeholder informationer, der er klassificeret højere end RESTREINT UE/EU RESTRICTED

b) medmindre den pågældende medlemsstats NSA anmoder om, at der ikke foretages almindelig distribution, omdeles inspektionsrapporter til medlemmerne af Sikkerhedsudvalget og til ECSD; rapporten skal klassificeres som RESTREINT UE/EU RESTRICTED.

Der udarbejdes regelmæssigt en rapport under GSR's sikkerhedsmyndigheds (Sikkerhedskontorets) ansvar, som fremhæver erfaringerne fra de inspektioner, der er gennemført i medlemsstaterne i en nærmere angivet periode og behandlet af Sikkerhedsudvalget.

58. Med hensyn til vurderingsbesøg i tredjelande og internationale organisationer distribueres rapporten til Sikkerhedsudvalget og til ECSD. Rapporten skal mindst klassificeres som RESTREINT UE/EU RESTRICTED. Korrigerende foranstaltninger kontrolleres ved et opfølgningsbesøg og indberettes til Sikkerhedsudvalget.

59. Med hensyn til inspektioner af EU-agenturer og -organer nedsat i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union samt af Europol og Eurojust distribueres inspektionsrapporten til medlemmerne af Sikkerhedsudvalget og til ECSD. Udkastet til inspektionsrapport fremsendes til vedkommende agentur eller organ for at kontrollere, at den er faktuelt korrekt, og at den ikke indeholder informationer, der er klassificeret højere end RESTREINT UE/EU RESTRICTED. Korrigerende foranstaltninger kontrolleres ved et opfølgningsbesøg og indberettes til Sikkerhedsudvalget.

60. GSR's sikkerhedsmyndighed gennemfører regelmæssigt inspektioner af organisatoriske enheder i GSR med de formål, der er fastlagt i punkt 48.

Inspektionscheckliste

61. GSR's sikkerhedsmyndighed (Sikkerhedskontoret) udarbejder og ajourfører en sikkerhedsinspektionscheckliste for de punkter, der skal kontrolleres under en inspektion. Denne checkliste fremsendes til Sikkerhedsudvalget.

62. Oplysninger til brug for checklisten indhentes, navnlig under inspektionen, hos de ledende sikkerhedsansvarlige i den enhed, der inspiceres. Når checklisten er udfyldt med de detaljerede svar, klassificeres den efter aftale med den inspicerede enhed. Den indgår ikke i inspektionsrapporten.

BILAG IV

BESKYTTELSE AF EUCI, DER HÅNDTERES I CIS'ER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 10.

2. Følgende IA-egenskaber og -koncepter er væsentlige for sikkerheden og for, at operationer i CIS'er kan fungere korrekt:

autenticitet:	sikkerhed for, at informationer er ægte og fra bona fide-kilder
tilgængelighed:	det forhold, at informationer er tilgængelige og kan anvendes på anmodning af en autoriseret enhed
fortrolighed:	det forhold, at informationer ikke videregives til uautoriserede personer, enheder eller processer
integritet:	sikring af informationernes og aktivernes rigtighed og fuldstændighed
uafviselighed:	evnen til at bevise, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes.

II. INFORMATIONSSIKRINGSPRINCIPPER

3. Nedenstående bestemmelser er grundlaget for sikkerhedsbeskyttelse af al håndtering af EUCI i CIS'er. Detaljerede krav til gennemførelse af disse bestemmelser defineres i sikkerhedspolitikker og sikkerhedsretningslinjer for informationssikring.

Sikkerhedsrisikostyring

4. Sikkerhedsrisikostyringen skal være en integrerende del af at fastlægge, udvikle, drive og opretholde CIS'er. Risikostyringen (vurdering, behandling, accept og kommunikation) skal foregå som en gentagelsesproces, der gennemføres i fællesskab af repræsentanter for systemejere, projektmyndigheder, driftsmyndigheder og sikkerhedsgodkendelsesmyndigheder under anvendelse af en gennemprøvet, gennemsigtig og fuldt forståelig risikovurderingsproces. Anvendelsesområdet for CIS'et og dets aktiver skal klart defineres fra starten af risikostyringsprocessen.

5. De kompetente myndigheder skal tage de potentielle trusler mod CIS'er op til revision og opretholde ajourførte og præcise trusselvurderinger, der afspejler det aktuelle operative miljø. De skal hele tiden ajourføre deres viden om spørgsmål i forbindelse med sårbarhed og regelmæssigt tage sårbarhedsvurderingen op til revision med afsæt i et informationsteknologimiljø (it-miljø) i stadig forandring.

6. Formålet med sikkerhedsrisikobehandling er at anvende et sæt sikkerhedsforanstaltninger, der giver sig udslag i en tilfredsstillende balance mellem brugerkrav, omkostninger og residualrisiko.

7. De specifikke krav og det detaljeringsomfang og den detaljeringsgrad, der fastlægges af den relevante SAA for akkreditering af et CIS, skal svare til den vurderede risiko under hensyntagen til alle relevante faktorer, herunder klassifikationsgraden af de EUCI, der håndteres i CIS'et. Akkreditering skal omfatte en formel udredning om residualrisikoen og en ansvarlig myndigheds accept af residualrisikoen.

Sikkerhed i hele CIS'ets livscyklus

8. Opretholdelse af sikkerheden skal være et krav i hele CIS'ets livscyklus fra startfasen til udtagningen af drift.

9. Den rolle, som hver enkelt aktør i et CIS spiller, og dens interaktion med hensyn til sikkerhed skal fastlægges for hver fase af livscyklussen.

10. Ethvert CIS, herunder dets tekniske og ikke-tekniske sikkerhedsforanstaltninger, er underkastet afprøvning af sikkerheden under akkrediteringsprocessen for at sikre, at det relevante sikkerhedsniveau er nået, og kontrollere, at de er korrekt implementeret, integreret og konfigureret.

11. Der skal regelmæssigt udføres sikkerhedsvurderinger, -inspektioner og -revisioner under driften og vedligeholdelsen af et CIS, og når der opstår ekstraordinære omstændigheder.

12. Sikkerhedsdokumentationen for et CIS skal udvikles i løbet af dets livscyklus som en integrerende del af ændrings- og konfigurationsstyringsprocessen.

Bedste praksis

13. GSR og medlemsstaterne samarbejder om at udvikle bedste praksis for sikkerhedsbeskyttelse af EUCI, der håndteres i CIS'er. Retningslinjerne for bedste praksis skal omfatte de tekniske, fysiske, organisatoriske og proceduremæssige sikkerhedsforanstaltninger for CIS'er, som bevisligt er effektive med hensyn til imødegåelse af trusler og sårbarheder.

14. Sikkerhedsbeskyttelsen af EUCI, der håndteres i CIS'er, skal trække på de erfaringer, som enheder involveret i IA både inden for og uden for EU har gjort.

15. Udbredelsen og den efterfølgende gennemførelse af bedste praksis skal bidrage til at nå et ækvivalent sikringsniveau for de forskellige CIS'er, der drives af GSR og af medlemsstater, der håndterer EUCI.

Dybdeforsvar

16. For at afbøde risikoen i forbindelse med CIS'er skal der gennemføres en række tekniske og ikke-tekniske sikkerhedsforanstaltninger, der er organiseret som en kæde af forsvarsmekanismer. Denne kæde skal omfatte:

a) *afskrækkelse:* sikkerhedsforanstaltninger med det formål at afskrække fjendtlig planlægning af angreb på CIS'er

b) *forebyggelse:* sikkerhedsforanstaltninger med det formål at hindre eller blokere angreb på CIS'er

c) *afsløring:* sikkerhedsforanstaltninger med det formål at opdage angreb på CIS'er

d) *modstandsdygtighed:* sikkerhedsforanstaltninger med det formål at begrænse virkningerne af et angreb til et minimum af informationer eller CIS-aktiver og afværge yderligere skade og

e) *genopretning:* sikkerhedsforanstaltninger med det formål at genoprette en sikker situation for CIS'er.

Det skal afgøres ved en risikovurdering, hvor strenge disse tekniske sikkerhedsforanstaltninger skal være.

17. De kompetente myndigheder skal sikre, at de kan imødegå hændelser, der kan overskride organisatoriske og nationale grænser, med henblik på at koordinere svar og udveksle informationer om disse hændelser og den hermed forbundne risiko (edb-nødberedskabskapaciteter).

Minimalisme- og »least privilege«-princippet

18. Der implementeres kun de funktioner, det udstyr og de tjenester, der er vigtigst for at opfylde operative behov og undgå unødvendige risici.

19. CIS-brugere og automatiserede processer skal kun gives den adgang, de privilegier eller de autorisationer, de har behov for til at udføre deres opgaver, med henblik på at begrænse enhver skade, der kan opstå ved uheld, fejl eller uautoriseret brug af CIS-ressourcer.

20. De registreringsprocedurer, der udføres af et CIS, skal, hvor det er nødvendigt, kontrolleres som led i akkrediteringsprocessen.

Bevidsthed om informationssikring (IA)

21. Den første forsvarslinje for CIS'ers sikkerhed er, at der er bevidsthed om risiciene, og at der findes sikkerhedsforanstaltninger. Det er navnlig nødvendigt, at alt det personale, der er involveret i CIS'ers livscyklus, herunder brugerne, forstår:

a) at sikkerhedssvigt i betydelig grad kan skade CIS'er

b) den potentielle skade mod andre, som kan opstå på grund af sammenkobling og indbyrdes afhængighed, og

c) at de hver især har et ansvar og ansvarliggøres for CIS'ers sikkerhed afhængigt af deres roller inden for systemerne og processerne.

22. For at sikre, at sikkerhedsansvaret forstås, skal IA-uddannelse og -bevidsthedstræning være obligatorisk for alt berørt personale, herunder ledere og CIS-brugere.

Evaluering og godkendelse af it-sikkerhedsprodukter

23. Den nødvendige grad af tillid til sikkerhedsforanstaltningerne, defineret som et sikringsniveau, fastlægges i overensstemmelse med resultatet af risikostyringsprocessen og med de relevante sikkerhedspolitikker og sikkerhedsretningslinjer.

24. Sikringsniveauet efterprøves ved at anvende internationalt anerkendte eller nationalt godkendte processer og metoder. Dette omfatter primært evaluering, kontrol og revision.

25. Kryptoprodukter til sikkerhedsbeskyttelse af EUCI skal først evalueres og godkendes af en national CAA i en medlemsstat.

26. Inden de kan anbefales til godkendelse af Rådet eller generalsekretæren i overensstemmelse med artikel 10, stk. 6, skal sådanne kryptoprodukter undergå en andenpartsevaluering med positivt resultat foretaget af en kvalificeret evalueringsmyndighed (AQUA) i en medlemsstat, der ikke medvirker til at designe eller fremstille udstyret. Hvor detaljeret andenpartsevalueringen skal være, afhænger af den planlagte højeste klassifikationsgrad for de EUCI, der skal beskyttes ved hjælp af disse produkter. Rådet skal godkende en sikkerhedspolitik for evaluering og godkendelse af kryptoprodukter.

27. Hvis det er berettiget af specifikke operative grunde, kan Rådet eller generalsekretæren, alt efter hvad der er relevant, efter henstilling fra Sikkerhedsudvalget dispensere fra kravene under punkt 25 eller 26 og udstede en midlertidig godkendelse for en specifik periode efter proceduren i artikel 10, stk. 6.

28. En AQUA skal være en CAA i en medlemsstat, der på grundlag af kriterier, som er fastsat af Rådet, er blevet akkrediteret til at foretage andenpartsevalueringen af kryptoprodukter til beskyttelse af EUCI.

29. Rådet skal godkende en sikkerhedspolitik for kvalifikation og godkendelse af ikke-kryptografiske it-sikkerhedsprodukter.

Transmission inden for sikrede områder

30. Ved transmission af EUCI inden for sikrede områder kan ukrypteret distribution eller kryptering på et lavere niveau anvendes på grundlag af resultatet af en risikostyringsproces og med forbehold af godkendelse fra SAA'en, jf. dog bestemmelserne i denne afgørelse.

Sikker sammenkobling af CIS'er

31. I denne afgørelse forstås ved systemsammenkobling direkte kobling af to eller flere it-systemer med henblik på udveksling af data og andre informationsressourcer (f.eks. kommunikation) i en eller flere retninger.

32. Et CIS skal behandle et tilkoblet it-system som upålideligt og gennemføre beskyttelsesforanstaltninger for at kontrollere udvekslingen af klassificerede informationer.

33. For alle sammenkoblinger af et CIS med et andet it-system skal følgende grundlæggende krav opfyldes:

a) de forretningsmæssige eller operative krav til sådanne sammenkoblinger skal fastlægges og godkendes af de kompetente myndigheder

b) sammenkoblingen skal gennemgå en risikostyrings- og akkrediteringsproces og godkendes af de kompetente SAA'er, og

c) der skal oprettes grænsebeskyttelsestjenester (BPS) rundt om alle CIS'er.

34. Der må ikke være nogen sammenkobling mellem et akkrediteret CIS og et ubeskyttet eller offentligt netværk, medmindre CIS'et har godkendt den BPS, der er installeret til dette formål mellem CIS'et og det ubeskyttede eller offentlige netværk. Sikkerhedsforanstaltningerne for sådanne sammenkoblinger skal tages op til revision af den kompetente IAA og godkendes af den kompetente SAA.

Hvis det ubeskyttede eller offentlige netværk udelukkende anvendes som bærer, og dataene er krypteret ved hjælp af et kryptoprodukt, som er godkendt i overensstemmelse med artikel 10, anses forbindelsen ikke for at være en sammenkobling.

35. Direkte sammenkobling eller kaskadekobling mellem et CIS, der er godkendt til at håndtere informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, og et ubeskyttet eller offentligt netværk er forbudt.

Edb-lagringsmedier

36. Edb-lagringsmedier skal destrueres i overensstemmelse med procedurer, der er godkendt af den kompetente sikkerhedsmyndighed.

37. Edb-lagringsmedier skal genanvendes, nedklassificeres eller afklassificeres i overensstemmelse med en sikkerhedspolitik, der skal fastlægges i henhold til artikel 6, stk. 1.

Nødsituationer

38. Uanset bestemmelserne i denne afgørelse kan de særlige procedurer, der er beskrevet i det følgende, anvendes i en nødsituation, f.eks. under forestående eller faktiske krise-, konflikt- eller krigssituationer eller under ekstraordinære operative forhold.

39. EUCI kan transmitteres ved hjælp af kryptoprodukter, der er godkendt til en lavere klassifikationsgrad, eller endog ukrypteret med den kompetente myndigheds godkendelse, hvis enhver forsinkelse ville forvolde en skade, der er langt alvorligere end den skade, som videregivelse af det klassificerede materiale ville forvolde, og hvis:

a) afsender og modtager ikke har de krævede krypteringsmidler eller slet ingen krypteringsmidler, og

b) det klassificerede materiale ikke kan sendes i tide med andre midler.

40. Klassificerede informationer, der transmitteres under de i punkt 38 nævnte omstændigheder, må ikke bære nogen mærkning eller påtegning, der skiller dem ud fra informationer, der er uklassificeret eller kan beskyttes ved hjælp af et disponibelt kryptoprodukt. Modtagerne skal med andre midler straks underrettes om klassifikationsgraden.

41. Ved anvendelse af punkt 38 aflægges der efterfølgende rapport til den kompetente myndighed og Sikkerhedsudvalget.

III. INFORMATIONSSIKRINGSFUNKTIONER OG -MYNDIGHEDER

42. Følgende IA-funktioner skal etableres i medlemsstaterne og i GSR. Disse funktioner behøver ikke være organiseret i individuelle enheder. De skal have separate mandater. Disse funktioner og det medfølgende ansvar kan dog kombineres eller integreres i samme organisatoriske enhed eller opdeles i forskellige organisatoriske enheder, forudsat at det undgås, at der opstår interne interessekonflikter eller konflikter mellem arbejdsopgaver.

Informationssikringsmyndigheden (IA)

43. IAA'en er ansvarlig for:

a) udvikling af IA-sikkerhedspolitikker og sikkerhedsretningslinjer og overvågning af deres effektivitet og relevans

b) beskyttelse og forvaltning af tekniske informationer om kryptoprodukter

c) sikring af, at de IA-foranstaltninger, der vælges til sikkerhedsbeskyttelse af EUCI, er i overensstemmelse med de relevante politikker for deres egnethed og udvælgelse

d) sikring af, at kryptoprodukter udvælges i overensstemmelse med politikkerne for deres egnethed og udvælgelse

e) koordinering af IA-uddannelse og -bevidstgørelse

f) samarbejde med systemleverandøren, sikkerhedsaktørerne og brugerrepræsentanterne med hensyn til IA-sikkerhedspolitikkerne og sikkerhedsretningslinjerne, og

g) sikring af, at den relevante ekspertise er til rådighed i Sikkerhedsudvalgets ekspertunderudvalg vedrørende IA-spørgsmål.

Tempestmyndigheden

44. Tempestmyndigheden (TA) er ansvarlig for at sikre, at CIS'er er i overensstemmelse med Tempestpolitikkerne og -retningslinjerne. Den skal godkende Tempestmodforanstaltninger vedrørende anlæg og produkter til beskyttelse af EUCI til en bestemt klassifikationsgrad i det operative miljø.

Kryptogodkendelsesmyndigheden

45. Kryptogodkendelsesmyndigheden (CAA) er ansvarlig for at sikre, at kryptoprodukter er i overensstemmelse med den nationale kryptopolitik eller Rådets kryptopolitik. Den skal godkende et kryptoprodukt til beskyttelse af EUCI til en bestemt klassifikationsgrad i det operative miljø. Med hensyn til medlemsstaterne er CAA desuden ansvarlig for at evaluere kryptoprodukter.

Kryptodistributionsmyndigheden

46. Kryptodistributionsmyndigheden (CDA) er ansvarlig for:

a) at forvalte og stå til regnskab for EU-kryptomateriale

b) at sikre, at der indføres og anvendes relevante procedurer og kanaler med henblik på at kunne stå til regnskab for alt EU-kryptomateriale og sikre dettes håndtering, opbevaring og distribution, og

c) at sikre overdragelse af EU-kryptomateriale til eller fra enkeltpersoner eller tjenester, der bruger det.

Sikkerhedsakkrediteringsmyndigheden

47. Sikkerhedsakkrediteringsmyndigheden (SAA) for hvert system er ansvarlig for:

a) at sikre, at CIS'er overholder de relevante sikkerhedspolitikker og sikkerhedsretningslinjer, at give en udredning om godkendelse af CIS'er til håndtering af EUCI med en bestemt klassifikationsgrad i det operative miljø og at angive betingelserne for akkrediteringen og kriterierne for fornyet godkendelse

b) etablering af en sikkerhedsakkrediteringsproces i overensstemmelse med de relevante politikker, der klart angiver de godkendelsesbetingelser, der gælder for et CIS under dens ansvar

c) definition af en sikkerhedsakkrediteringsstrategi, der fastsætter en detaljeringsgrad for akkrediteringsprocessen svarende til det krævede sikringsniveau

d) gennemgang og godkendelse af sikkerhedsrelateret dokumentation, herunder udredninger om risikostyring og residualrisiko, systemspecifikke sikkerhedskrav (i det følgende benævnt »SSRS«), dokumentation for kontrol af sikkerhedsimplementering og operationelle sikkerhedsprocedurer (i det følgende benævnt »SecOPs«), og sikring af, at den er i overensstemmelse med Rådets sikkerhedsregler og sikkerhedspolitik

e) kontrol af implementeringen af sikkerhedsforanstaltningerne i forbindelse med CIS'et ved at foretage eller få foretaget sikkerhedsvurderinger, -inspektioner eller -revisioner

f) fastlæggelse af sikkerhedskrav (f.eks. niveauer for personelsikkerhedsgodkendelse) for CIS-følsomme stillinger

g) godkendelse af valget af godkendte krypto- og Tempestprodukter, der anvendes med henblik på at sikre et CIS

h) godkendelse af eller, hvor det er relevant, deltagelse i den fælles godkendelse af sammenkoblingen af et CIS med andre CIS'er, og

i) samarbejde med systemleverandøren, sikkerhedsaktørerne og brugerrepræsentanterne om sikkerhedsrisikostyring, især residualrisikoen, og betingelserne for godkendelseserklæringen.

48. GSR's SAA er ansvarlig for akkreditering af alle CIS'er, der anvendes inden for GSR's kompetenceområde.

49. En medlemsstats relevante SAA er ansvarlig for akkreditering af CIS'er og komponenter heraf, der anvendes inden for medlemsstatens kompetenceområde.

50. Et fælles sikkerhedsakkrediteringsudvalg (SAB) er ansvarligt for akkreditering af CIS'er, der både henhører under GSR's SAA og medlemsstaternes SAA. Det består af en SAA-repræsentant fra hver medlemsstat med deltagelse af en SAA-repræsentant for Kommissionen. Andre enheder med knudepunkter i et CIS indbydes til at deltage, når det pågældende system drøftes.

SAB har en repræsentant for GSR's SAA som formand. Det træffer afgørelse ved konsensus blandt SAA-repræsentanterne for institutioner, medlemsstater og andre enheder med knudepunkter i CIS'et. Det aflægger regelmæssigt rapport om sine aktiviteter til Sikkerhedsudvalget og meddeler det alle akkrediteringsudredninger.

Den operative informationssikringsmyndighed

51. Den operative IA-myndighed for hvert system er ansvarlig for:

a) udvikling af sikkerhedsdokumentation i overensstemmelse med sikkerhedspolitikkerne og sikkerhedsretningslinjerne, især SSRS, herunder udredningen om residualrisikoen, SecOPs og kryptoplanen inden for CIS-akkrediteringsprocessen

b) deltagelse i udvælgelse og afprøvning af systemspecifikke tekniske sikkerhedsforanstaltninger, -anordninger og -software for at overvåge deres implementering og for at sikre, at de installeres, konfigureres og vedligeholdes sikkert i overensstemmelse med den relevante sikkerhedsdokumentation

c) deltagelse i udvælgelse af Tempestsikkerhedsforanstaltninger og -anordninger, hvis det kræves i SSRS, og sikring af, at de installeres og vedligeholdes sikkert i samarbejde med TA

d) overvågning af gennemførelse og anvendelse af SecOps og, hvor det er relevant, uddelegering af operationelt sikkerhedsansvar til systemejeren

e) forvaltning og håndtering af kryptoprodukter, sikker opbevaring af kryptomateriale og kontrolleret materiale og om nødvendigt generering af kryptovariabler

f) gennemførelse af sikkerhedsanalyserevisioner og -afprøvninger, især for at udarbejde relevante risikorapporter, som krævet af SAA

g) CIS-specifik IA-uddannelse

h) implementering og anvendelse af CIS-specifikke sikkerhedsforanstaltninger.

BILAG V

INDUSTRISIKKERHED

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 11. Det fastsætter generelle sikkerhedsbestemmelser, der er gældende for industrivirksomheder eller andre enheder under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter, der tildeles af GSR.

2. Rådet godkender en politik for industrisikkerhed, der navnlig indeholder detaljerede krav vedrørende FSC'er, de særlige sikkerhedsbetingelser (SAL), besøg, transmission og transport af EUCI.

II. SIKKERHEDSELEMENTER I EN KLASSIFICERET KONTRAKT

Klassifikationsvejledning (SCG)

3. Inden der iværksættes et udbud eller tildeles en klassificeret kontrakt, skal GSR som kontraherende myndighed fastsætte klassifikationsgraden for informationer, som skal videregives til bydende og kontrahenter, samt klassifikationsgraden for informationer, som kontrahenten skal udarbejde. Med henblik herpå udarbejder GSR en SCG, der skal anvendes ved opfyldelsen af kontrakten.

4. For at fastlægge klassifikationsgraden for de forskellige elementer i en klassificeret kontrakt anvendes følgende principper:

   a) ved udarbejdelsen af en SCG skal GSR tage hensyn til alle relevante sikkerhedsaspekter, herunder den klassifikationsgrad, der er tildelt informationer, som udstederen af informationerne har videregivet og godkendt til brug for kontrakten

   b) kontraktens samlede klassifikationsgrad kan ikke være lavere end den højeste klassifikationsgrad for dens enkelte elementer, og

   c) GSR skal, når det er relevant, samarbejde med medlemsstaternes NSA'er/DSA'er eller anden berørt kompetent sikkerhedsmyndighed, hvis der skal foretages ændringer i klassifikationen af informationer, der er udarbejdet af eller videregivet til kontrahenter i forbindelse med opfyldelsen af en kontrakt, og når der foretages eventuelle yderligere ændringer af SCG.

Særlige sikkerhedsbetingelser (SAL)

5. Sikkerhedskravene for de enkelte kontrakter beskrives i SAL. SAL skal, når det er relevant, indeholde SCG og skal være en integrerende del af en klassificeret kontrakt eller underkontrakt.

6. SAL skal indeholde bestemmelser om, at kontrahenten og/eller underkontrahenten skal opfylde minimumsstandarderne i denne afgørelse. Manglende overholdelse af minimumsstandarderne kan udgøre en tilstrækkelig grund til, at kontrakten ophæves.

Program-/projektsikkerhedsinstruktion (PSI)

7. Afhængigt af omfanget af programmer eller projekter, der kræver adgang til eller håndtering eller opbevaring af EUCI, kan den kontraherende myndighed, der er udpeget til at forvalte programmet eller projektet, udarbejde specifikke program-/projektsikkerhedsinstruktioner (PSI). PSI kræver godkendelse fra medlemsstaternes NSA'er/DSA'er eller anden berørt kompetent sikkerhedsmyndighed, der deltager i programmet/projektet, og kan indeholde yderligere sikkerhedskrav.

III. FACILITETSSIKKERHEDSGODKENDELSE (FSC)

8. En FSC meddeles af en medlemsstats NSA eller DSA eller anden kompetent sikkerhedsmyndighed som angivelse af, at en industrivirksomhed eller anden enhed i overensstemmelse med nationale love og bestemmelser kan sikkerhedsbeskytte EUCI med den relevante klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) inden for sine faciliteter. Den skal forelægges for GSR som kontraherende myndighed, inden en kontrahent eller underkontrahent eller en potentiel kontrahent eller underkontrahent kan få rådighed over eller tildeles adgang til EUCI.

9. Den relevante NSA eller DSA skal ved meddelelsen af en FSC som minimum:

   a) evaluere industrivirksomhedens eller en anden enheds integritet

   b) evaluere ejerskab, kontrol eller mulighed for uretmæssig påvirkning, der kan betragtes som en sikkerhedsrisiko

c) kontrollere, at industrivirksomheden eller en anden enhed har indført et sikkerhedssystem inden for faciliteten, der omfatter alle relevante sikkerhedsforanstaltninger, der er nødvendige for at beskytte informationer eller materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i overensstemmelse med kravene i denne afgørelse

d) kontrollere, at der for ledere, ejere og ansatte, der skal have adgang til informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, er blevet fastlagt en personelsikkerhedsstatus i overensstemmelse med kravene i denne afgørelse

e) kontrollere, at industrivirksomheden eller en anden enhed har udpeget en facilitetssikkerhedsofficer, der over for ledelsen er ansvarlig for håndhævelsen af de sikkerhedsmæssige forpligtelser i den pågældende enhed.

10. Når det er relevant, underretter GSR som kontraherende myndighed den relevante NSA/DSA eller anden kompetent sikkerhedsmyndighed om, at der er behov for en FSC i perioden forud for indgåelse af en kontrakt eller med henblik på opfyldelsen af en kontrakt. En FSC eller PSC er påkrævet i perioden forud for indgåelsen af en kontrakt, hvis EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal videregives i løbet af udbudsproceduren.

11. Den kontraherende myndighed tildeler ikke en klassificeret kontrakt til en udvalgt bydende, før den fra NSA'en/DSA'en eller anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor den pågældende kontrahent eller underkontrahent er registreret, har fået bekræftet, at den relevante FSC, hvor det er påkrævet, er udstedt.

12. Den NSA/DSA eller anden kompetent sikkerhedsmyndighed, der har udstedt en FSC, skal underrette GSR som kontraherende myndighed om ændringer, der berører FSC'en. I tilfælde af en underkontrakt underrettes NSA'en/DSA'en eller anden kompetent sikkerhedsmyndighed tilsvarende.

13. Hvis den relevante NSA/DSA eller anden kompetent sikkerhedsmyndighed inddrager en FSC, er det en tilstrækkelig grund til, at GSR som kontraherende myndighed ophæver en klassificeret kontrakt eller udelukker en bydende fra udvælgelsen.

IV. KLASSIFICEREDE KONTRAKTER OG UNDERKONTRAKTER

14. Hvis EUCI videregives til en bydende i perioden forud for indgåelsen af en kontrakt, skal udbudsbekendtgørelsen indeholde en bestemmelse, der forpligter den bydende, der undlader at afgive bud, eller som ikke udvælges, til at returnere alle klassificerede dokumenter inden for en bestemt tidsfrist.

15. Når der er tildelt en klassificeret kontrakt eller underkontrakt, underretter GSR som kontraherende myndighed kontrahentens eller underkontrahentens NSA/DSA eller anden kompetent sikkerhedsmyndighed om sikkerhedsbestemmelserne for den klassificerede kontrakt.

16. Når sådanne kontrakter ophæves, underretter GSR som kontraherende myndighed (og/eller NSA'en/DSA'en eller anden kompetent sikkerhedsmyndighed i tilfælde af en underkontrakt, alt efter hvad der er hensigtsmæssigt,) straks NSA'en/DSA'en eller anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor kontrahenten eller underkontrahenten er registreret.

17. Som hovedregel er kontrahenten eller underkontrahenten forpligtet til at returnere EUCI, som vedkommende er i besiddelse af, til den kontraherende myndighed ved ophævelsen af den klassificerede kontrakt eller underkontrakt.

18. De særlige bestemmelser for bortskaffelse af EUCI under opfyldelsen af kontrakten eller ved dens ophævelse fastsættes i SAL.

19. Er kontrahenten eller underkontrahenten autoriseret til at beholde EUCI efter kontraktens ophævelse, skal minimumsstandarderne i denne afgørelse fortsat opfyldes, og kontrahenten eller underkontrahenten skal beskytte EUCI's fortrolighed.

20. De betingelser, hvorpå kontrahenten kan udbyde dele af kontrakten i underentreprise, skal fastsættes i udbuddet og i kontrakten.

21. En kontrahent skal indhente tilladelse fra GSR som kontraherende myndighed, inden en del af en klassificeret kontrakt udbydes i underentreprise. En underkontrakt må ikke tildeles industrivirksomheder eller andre enheder, som er registreret i et tredjeland, der ikke har indgået en informationssikkerhedsaftale med EU.

22. Kontrahenten er ansvarlig for at sikre, at alle underkontraheringsaktiviteter gennemføres i overensstemmelse med minimumsstandarderne i denne afgørelse, og må ikke videregive EUCI til en underkontrahent uden forudgående skriftligt samtykke fra den kontraherende myndighed.

23. For så vidt angår EUCI, der udarbejdes eller håndteres af kontrahenten eller underkontrahenten, varetager den kontraherende myndighed udsteders rettigheder.

V. BESØG I FORBINDELSE MED KLASSIFICEREDE KONTRAKTER

24. Hvis GSR, kontrahenter eller underkontrahenter skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, i hinandens lokaliteter med henblik på opfyldelse af en klassificeret kontrakt, skal der tilrettelægges besøg i samråd med de pågældende NSA'er/DSA'er eller anden berørt kompetent sikkerhedsmyndighed. I forbindelse med specifikke projekter kan NSA'en/DSA'en dog også aftale en procedure, hvorved sådanne besøg kan tilrettelægges direkte.

25. Alle besøgende skal være i besiddelse af en relevant PSC og have need-to-know med henblik på adgang til EUCI vedrørende kontrakten med GSR.

26. Besøgende kan kun få adgang til EUCI, der har relation til besøgets formål.

VI. TRANSMISSION OG TRANSPORT AF EUCI

27. For så vidt angår elektronisk transmission af EUCI anvendes de relevante bestemmelser i artikel 10 og bilag IV.

28. For så vidt angår transport af EUCI anvendes de relevante bestemmelser i bilag III til denne afgørelse i overensstemmelse med nationale love og bestemmelser.

29. For så vidt angår fragttransport af klassificeret materiale anvendes følgende principper ved fastlæggelsen af sikkerhedsordninger:

a) sikkerheden skal garanteres på alle stadier under transporten fra udgangspunktet til det endelige bestemmelsessted

b) den beskyttelsesgrad, der skal tillægges en forsendelse, bestemmes af den højeste klassifikationsgrad for det materiale, den indeholder

c) transportvirksomhederne skal have en FSC på det rette niveau. I sådanne tilfælde skal medarbejdere, der håndterer forsendelsen, være sikkerhedsgodkendt i overensstemmelse med bilag I

d) forud for enhver grænseoverskridende transport af materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, udarbejder afsenderen en transportplan, som godkendes af den pågældende NSA/DSA eller anden berørt kompetent sikkerhedsmyndighed

e) transporten gennemføres så vidt muligt direkte og afsluttes så hurtigt, som forholdene tillader

f) ruterne bør så vidt muligt kun gå gennem medlemsstater. Der bør kun benyttes ruter gennem andre lande end medlemsstater, hvis NSA'en/DSA'en eller anden kompetent sikkerhedsmyndighed i såvel afsenderens som modtagerens stat har givet tilladelse hertil.

VII. VIDEREGIVELSE AF EUCI TIL KONTRAHENTER I TREDJELANDE

30. EUCI videregives til kontrahenter og underkontrahenter i tredjelande i overensstemmelse med de sikkerhedsforanstaltninger, der er aftalt mellem GSR som kontraherende myndighed og NSA'en/DSA'en i det pågældende tredjeland, hvor kontrahenten er registreret.

VIII. HÅNDTERING OG OPBEVARING INFORMATIONER, DER ER KLASSIFICERET RESTREINT UE/EU RESTRICTED

31. Sammen med medlemsstatens NSA/DSA, alt efter hvad der er hensigtsmæssigt, har GSR som kontraherende myndighed ret til at besøge kontrahenters/underkontrahenters faciliteter på grundlag af kontraktbestemmelser for at kontrollere, at de relevante sikkerhedsforanstaltninger til beskyttelse af EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, er iværksat som krævet ifølge kontrakten.

32. I det omfang, det er nødvendigt i henhold til nationale love og bestemmelser, underrettes NSA'er/DSA'er eller anden kompetent sikkerhedsmyndighed af GSR som den kontraherende myndighed om kontrakter eller underkontrakter, der indeholder informationer, der er klassificeret RESTREINT UE/EU RESTRICTED.

33. En FSC eller en PSC til kontrahenter eller underkontrahenter og deres personale er ikke påkrævet for kontrakter, der tildeles af GSR og indeholder informationer, som er klassificeret RESTREINT UE/EU RESTRICTED.

34. GSR undersøger som kontraherende myndighed svarene på udbud vedrørende kontrakter, der kræver adgang til informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, uanset de krav med hensyn til FSC eller PSC, der måtte findes i nationale love og bestemmelser.

35. De betingelser, hvorpå kontrahenten kan udbyde dele af kontrakten i underentreprise, skal være i overensstemmelse med punkt 21.

36. Hvis en kontrakt omfatter håndtering af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, i et CIS, som drives af en kontrahent, sikrer GSR som kontraherende myndighed, at kontrakten eller underkontrakten nærmere beskriver de nødvendige tekniske og administrative krav for akkreditering af CIS'et, som svarer til den vurderede risiko, under hensyntagen til alle relevante faktorer. Omfanget af akkrediteringen af et CIS aftales mellem den kontraherende myndighed og den relevante NSA/DSA.

BILAG VI

UDVEKSLING AF KLASSIFICEREDE INFORMATIONER MED TREDJELANDE OG INTERNATIONALE ORGANISATIONER

I. INDLEDNING

1. Dette bilag indeholder bestemmelser til gennemførelse af artikel 12.

II. RAMMER FOR UDVEKSLING AF KLASSIFICEREDE INFORMATIONER

2. Hvis Rådet beslutter, at der er et langsigtet behov for udveksling af klassificerede informationer,

— indgås der en informationssikkerhedsaftale, eller

— indgås der en administrativ ordning

i overensstemmelse med artikel 12, stk. 2, og afsnit III og IV og på grundlag af en henstilling fra Sikkerhedsudvalget.

3. Hvis EUCI, der er udarbejdet med henblik på en FSFP-operation, skal videregives til tredjelande eller internationale organisationer, der deltager i en sådan operation, og hvis ingen af rammerne i punkt 2 findes, reguleres udvekslingen af EUCI med det deltagende tredjeland eller den deltagende internationale organisation, i overensstemmelse med afsnit V, i:

— en rammeaftale om deltagelse

— en ad hoc-aftale om deltagelse, eller

— hvis der ikke findes nogen af ovennævnte, en administrativ ad hoc-ordning.

4. Hvis der ikke findes en ramme som omhandlet i punkt 2 og 3 og i tilfælde, hvor det besluttes at videregive EUCI til et tredjeland eller en international organisation på et ekstraordinært ad hoc-grundlag, jf. afsnit VI, indhentes der skriftlig garanti fra det pågældende tredjeland eller den pågældende internationale organisation for at sikre, at det/den beskytter de EUCI, der videregives, i overensstemmelse med grundprincipperne og minimumsstanderne i denne afgørelse.

III. INFORMATIONSSIKKERHEDSAFTALER

5. Informationssikkerhedsaftaler skal fastlægge grundprincipperne og minimumsstandarderne for udveksling af klassificerede informationer mellem EU og et tredjeland eller en international organisation.

6. Informationssikkerhedsaftaler skal indeholde bestemmelser om tekniske gennemførelsesordninger, der aftales mellem GSR's Sikkerhedskontor, ECSD og den kompetente sikkerhedsmyndighed i det pågældende tredjeland eller den pågældende internationale organisation. Ordningerne skal tage hensyn til beskyttelsesniveauet i de sikkerhedsforskrifter, -strukturer og -procedurer, der findes i tredjelandet eller den internationale organisation. De skal godkendes af Sikkerhedsudvalget.

7. EUCI må ikke udveksles elektronisk, medmindre det udtrykkeligt er fastsat i informationssikkerhedsaftalen eller de tekniske gennemførelsesordninger.

8. Informationssikkerhedsaftaler skal fastsætte, at GSR's Sikkerhedskontor og ECSD inden udvekslingen af klassificerede informationer i henhold til aftalen skal være enige om, at den modtagende part vil kunne beskytte og sikre de informationer, der videregives, på en passende måde.

9. Når Rådet indgår en informationssikkerhedsaftale, udpeges en registratur hos hver part som hovedkanal for ind- og udgående udveksling af klassificerede informationer.

10. For at vurdere effektiviteten af sikkerhedsforskrifterne, -strukturerne og -procedurerne i det pågældende tredjeland eller den pågældende internationale organisation gennemfører GSR's Sikkerhedskontor sammen med ECSD vurderingsbesøg efter fælles aftale med tredjelandet eller den internationale organisation. Vurderingsbesøg gennemføres i overensstemmelse med de relevante bestemmelser i bilag III, og følgende evalueres:

a) de reguleringsmæssige rammer for sikkerhedsbeskyttelsen af klassificerede informationer

b) særlige kendetegn ved sikkerhedspolitikken og den måde, hvorpå sikkerheden er organiseret i tredjelandet eller den internationale organisation, der kan få indflydelse på klassifikationsgraden for de informationer, der kan udveksles

c) de sikkerhedsforanstaltninger og -procedurer, der reelt er indført, og

d) sikkerhedsgodkendelseprocedurerne i forbindelse med klassifikationsgraden for de EUCI, der skal videregives.

11. Det hold, der gennemfører et vurderingsbesøg på vegne af EU, skal vurdere, om sikkerhedsforskrifterne og -procedurerne i det pågældende tredjeland eller den pågældende internationale organisation er tilstrækkelige med henblik på beskyttelse af EUCI med en bestemt klassifikationsgrad.

12. Resultaterne af sådanne besøg beskrives i en rapport, som danner grundlag for Sikkerhedsudvalgets beslutning om den højeste klassifikationsgrad for de EUCI, der kan udveksles i papirform og, hvis det er relevant, elektronisk med den berørte tredjepart, samt eventuelle særlige betingelser for udveksling med denne part.

13. Alle bestræbelser skal sættes ind på at gennemføre et fuldt sikkerhedsvurderingsbesøg til det pågældende tredjeland eller den pågældende internationale organisation, inden Sikkerhedsudvalget godkender gennemførelsesordningerne, med henblik på at fastslå arten og effektiviteten af det sikkerhedssystem, der forefindes. Hvis dette imidlertid ikke er muligt, skal Sikkerhedsudvalget modtage så fuldstændig en rapport som muligt fra GSR's Sikkerhedskontor, baseret på de informationer, det råder over, der orienterer Sikkerhedsudvalget om de sikkerhedsforskrifter, der anvendes, og om den måde, hvorpå sikkerheden er organiseret i tredjelandet eller den internationale organisation.

14. Sikkerhedsudvalget kan beslutte, at EUCI, indtil man har gennemgået resultatet af vurderingsbesøget, ikke må videregives eller kun må videregives op til en bestemt klassifikationsgrad, eller det kan fastsætte andre særlige betingelser for videregivelsen af EUCI til det pågældende tredjeland eller den pågældende internationale organisation. GSR's Sikkerhedskontor underretter tredjelandet eller den internationale organisation herom.

15. GSR's Sikkerhedskontor skal efter aftale med det pågældende tredjeland eller den pågældende internationale organisation jævnligt foretage opfølgende vurderingsbesøg for at kontrollere, at de indførte ordninger fortsat lever op til de aftalte minimumsstandarder.

16. Når informationssikkerhedsaftalen er i kraft, og der udveksles klassificerede informationer med det pågældende tredjeland eller den pågældende internationale organisation, kan Sikkerhedsudvalget beslutte at ændre den højeste klassifikationsgrad for de EUCI, der kan udveksles i papirform eller elektronisk, navnlig i lyset af opfølgende vurderingsbesøg.

IV. ADMINISTRATIVE ORDNINGER

17. Hvis der er et langsigtet behov for udveksling af informationer, der som hovedregel ikke må være klassificeret højere end RESTREINT UE/EU RESTRICTED, med et tredjeland eller en international organisation, og Sikkerhedsudvalget har fastslået, at den pågældende parts sikkerhedssystem ikke er tilstrækkelig udviklet til, at der kan indgås en informationssikkerhedsaftale, kan generalsekretæren, med forbehold af Rådets godkendelse, indgå en administrativ ordning med de relevante myndigheder i det pågældende tredjeland eller den pågældende internationale organisation.

18. Hvis der, af presserende operative grunde, er behov for hurtigt at etablere en ramme for udveksling af klassificerede informationer, kan Rådet undtagelsesvis beslutte, at der kan indgås en administrativ ordning for udveksling af informationer med en højere klassifikationsgrad.

19. Administrative ordninger skal som hovedregel have form af en brevveksling.

20. Der gennemføres et vurderingsbesøg som omhandlet i punkt 10, og rapporten fremsendes til Sikkerhedsudvalget, der skal vurdere den som tilfredsstillende, inden EUCI rent faktisk videregives til det pågældende tredjeland eller den pågældende internationale organisation. Hvis der foreligger ekstraordinære grunde til hurtig udveksling af klassificerede informationer, som Rådet orienteres om, kan EUCI dog videregives på betingelse af, at alle bestræbelser sættes ind på at foretage et sådant vurderingsbesøg hurtigst muligt.

21. EUCI må ikke udveksles elektronisk, medmindre det udtrykkeligt er fastsat i den administrative ordning.

V. UDVEKSLING AF KLASSIFICEREDE INFORMATIONER I FORBINDELSE MED FSFP-OPERATIONER

22. Rammeaftaler om deltagelse regulerer tredjelandes og internationale organisationers deltagelse i FSFP-operationer. Sådanne aftaler skal indeholde bestemmelser om videregivelse af EUCI, der er udarbejdet med henblik på FSFP-operationer, til de deltagende tredjelande eller internationale organisationer. Den højeste klassifikationsgrad for de EUCI, der kan udveksles, skal være RESTREINT UE/EU RESTRICTED for civile FSFP-operationer og CONFIDENTIEL UE/EU CONFIDENTIAL for militære FSFP-operationer, medmindre andet er fastlagt i afgørelsen om oprettelse af den enkelte FSFP-operation.

23. Ad hoc-aftaler om deltagelse, der indgås med henblik på en bestemt FSFP-operation, skal indeholde bestemmelser om videregivelse af EUCI, der er udarbejdet med henblik på den pågældende operation, til det deltagende tredjeland eller den deltagende internationale organisation. Den højeste klassifikationsgrad for de EUCI, der kan udveksles, skal være RESTREINT UE/EU RESTRICTED for civile FSFP-operationer og CONFIDENTIEL UE/EU CONFIDENTIAL for militære FSFP-operationer, medmindre andet er fastlagt i afgørelsen om oprettelse af den enkelte FSFP-operation.

24. Administrative ad hoc-ordninger om et tredjelands eller en international organisations deltagelse i en bestemt FSFP-operation kan bl.a. omfatte videregivelse af EUCI, der er udarbejdet med henblik på operationen, til det pågældende tredjeland eller den pågældende internationale organisation. Disse administrative ad hoc-ordninger indgås efter procedurerne i afsnit IV, punkt 17 og 18. Den højeste klassifikationsgrad for de EUCI, der kan udveksles, skal være RESTREINT UE/EU RESTRICTED for civile FSFP-operationer og CONFIDENTIEL UE/EU CONFIDENTIAL for militære FSFP-operationer, medmindre andet er fastlagt i afgørelsen om oprettelse af den enkelte FSFP-operation.

25. Ingen gennemførelsesordninger eller vurderingsbesøg er nødvendige, før bestemmelserne om videregivelse af EUCI som led i punkt 22, 23 og 24 gennemføres.

26. Hvis det værtsland, på hvis område en FSFP-operation gennemføres, ikke har nogen gældende informationssikkerhedsaftale eller administrativ ordning med EU for udveksling af klassificerede informationer, og der er et specifikt og øjeblikkeligt operativt behov, kan der indgås en administrativ ad hoc-ordning. Denne mulighed skal fastsættes i afgørelsen om oprettelse af FSFP-operationen. EUCI, der videregives under sådanne omstændigheder, skal begrænses til de informationer, der er udarbejdet med henblik på FSFP-operationen og højst er klassificeret RESTREINT UE/EU RESTRICTED. I henhold til en sådan administrativ ad hoc-ordning skal værtsstaten give tilsagn om at beskytte EUCI i overensstemmelse med minimumsstandarder, der mindst svarer til dem, der er fastlagt i denne afgørelse.

27. De bestemmelser om klassificerede informationer, der skal indgå i rammeaftaler om deltagelse, ad hoc-aftaler om deltagelse og administrative ad hoc-ordninger, jf. punkt 22-24, skal fastsætte, at det pågældende tredjeland eller den pågældende internationale organisation sikrer, at det personale, landet eller organisationen udstationerer til en given operation, vil beskytte EUCI i overensstemmelse med Rådets sikkerhedsregler og yderligere anvisninger udstedt af de kompetente myndigheder, herunder operationens kommandokæde.

28. Hvis der efterfølgende indgås en informationssikkerhedsaftale mellem EU og et deltagende tredjeland eller en deltagende international organisation, erstatter informationssikkerhedsaftalen enhver rammeaftale om deltagelse, ad hoc-aftale om deltagelse eller administrativ ad hoc-ordning, for så vidt angår udveksling og håndtering af EUCI.

29. Elektronisk udveksling af EUCI er ikke tilladt i henhold til en rammeaftale om deltagelse, en ad hoc-aftale om deltagelse eller en administrativ ad hoc-ordning med et tredjeland eller en international organisation, medmindre det udtrykkeligt er fastsat i den pågældende aftale eller ordning.

30. EUCI, der er udarbejdet med henblik på en FSFP-operation, kan videregives til personale, som tredjelande eller internationale organisationer har udstationeret til den pågældende operation i overensstemmelse med punkt 22-29. Når sådant personale autoriseres til at få adgang til EUCI i en FSFP-operations lokaliteter eller CIS'er, skal der træffes foranstaltninger til at afbøde risikoen for tab eller kompromittering (herunder registrering af de videregivne EUCI). Sådanne foranstaltninger defineres i relevante planlægnings- eller missionsdokumenter.

VI. EKSTRAORDINÆR AD HOC-VIDEREGIVELSE AF EUCI

31. Hvis der ikke er etableret en ramme i overensstemmelse med afsnit III-V, og Rådet eller et af dets forberedende organer beslutter, at der er et ekstraordinært behov for at videregive EUCI til et tredjeland eller en international organisation, skal GSR:

a) så vidt muligt, sammen med sikkerhedsmyndighederne i tredjelandet eller den internationale organisation kontrollere, at landets/organisationens sikkerhedsforskrifter, -strukturer og -procedurer er tilstrækkelige til at sikre, at de EUCI, der videregives, vil blive beskyttet efter standarder, der mindst svarer til dem, der er fastlagt i denne afgørelse

b) opfordre Sikkerhedsudvalget til på grundlag af de disponible oplysninger at udstede en henstilling vedrørende den tillid, der kan fæstes til sikkerhedsforskrifterne, -strukturerne og -procedurerne i det tredjeland eller den internationale organisation, som EUCI skal videregives til.

32. Hvis Sikkerhedsudvalget i sin henstilling går ind for at videregive EUCI, forelægges sagen for De Faste Repræsentanters Komité (Coreper), der træffer afgørelse om videregivelsen.

33. Hvis Sikkerhedsudvalget i sin henstilling ikke går ind for at videregive EUCI, sker følgende:

a) når der er tale om spørgsmål vedrørende FUSP/FSFP, drøfter Den Udenrigs- og Sikkerhedspolitiske Komité sagen og udfærdiger en henstilling til afgørelse, der træffes af Coreper

b) når der er tale om alle andre spørgsmål, drøfter Coreper sagen og træffer afgørelse.

34. Hvis det skønnes hensigtsmæssigt, kan Coreper med forbehold af forudgående skriftligt samtykke fra udstederen beslutte, at de klassificerede informationer kun må videregives delvist eller kun, hvis de forinden nedklassificeres eller afklassificeres, eller at de informationer, der skal videregives, skal udformes uden henvisning til kilden eller den oprindelige EU-klassifikationsgrad.

35. Hvis det besluttes at videregive EUCI, fremsender GSR det pågældende dokument med en videregivelsespåtegning, der angiver det tredjeland eller den internationale organisation, som informationerne er videregivet til. Inden eller ved den faktiske videregivelse skal den berørte tredjepart skriftligt give tilsagn om at beskytte de EUCI, den modtager, i overensstemmelse med de grundprincipper og minimumsstandarder, der er fastlagt i denne afgørelse.

VII. BEMYNDIGELSE TIL AT VIDEREGIVE EUCI TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

36. Hvis der findes en ramme som omhandlet i punkt 2 for udveksling af klassificerede informationer med et tredjeland eller en international organisation, træffer Rådet en afgørelse om bemyndigelse af generalsekretæren til i overensstemmelse med princippet om udstederens samtykke at videregive EUCI til det pågældende tredjeland eller den pågældende internationale organisation.

37. Hvis der findes en ramme som omhandlet i punkt 3 for udveksling af klassificerede informationer med et tredjeland eller en international organisation, er generalsekretæren bemyndiget til at videregive EUCI i overensstemmelse med afgørelsen om oprettelse af FSFP-operationen og med princippet om udstederens samtykke.

38. Generalsekretæren kan uddelegere sådanne bemyndigelser til ledende tjenestemænd i GSR eller andre personer under hans myndighed.

Tillæg

Tillæg A

DEFINITIONER

I denne afgørelse finder følgende definitioner anvendelse:

»afklassificering«: fjernelse af enhver sikkerhedsklassifikation

»akkreditering«: den proces, der fører til en formel erklæring fra sikkerhedsakkrediteringsmyndigheden (SAA) om, at et system er godkendt til at håndtere informationer med en bestemt klassifikationsgrad i en bestemt sikkerhedsindstilling i det operative miljø og på et acceptabelt risikoniveau baseret på, at der er gennemført en række godkendte tekniske, fysiske, organisatoriske og proceduremæssige sikkerhedsforanstaltninger.

»aktiv«: alt hvad der er af værdi for en organisation, dens forretningsmæssige drift og dennes kontinuitet, herunder informationsressourcer, der understøtter organisationens mission.

»certifikat for personelsikkerhedsgodkendelse« (PSCC): et certifikat udstedt af en kompetent myndighed, som fastslår, at en person er blevet sikkerhedsgodkendt og har en gyldig national PSC eller EU-PSC med den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), den relevante PSC's gyldighedsdato og certifikatets udløbsdato.

»CIS-livscyklus«: hele det tidsrum, et CIS eksisterer, hvilket indbefatter projektinitiering, idébeskrivelse, planlægning, kravanalyse, udformning, udvikling, afprøvning, implementering, drift og vedligeholdelse samt nedlæggelse.

»den, der er i besiddelse af«: en behørigt autoriseret person med en fastslået need-to-know-status, der er i besiddelse af EUCI og derfor er ansvarlig for at beskytte dem.

»dokument«: registrerede informationer uanset deres fysiske form eller karakteristika.

»dybdeforsvar«: anvendelse af en række sikkerhedsforanstaltninger, der er organiseret som en kæde af forsvarsmekanismer.

»EU's klassificerede informationer« (EUCI): se artikel 2, stk. 1.

»facilitetssikkerhedsgodkendelse« (FSC): en administrativ afgørelse truffet af en NSA eller DSA om, at en facilitet ud fra et sikkerhedsmæssigt synspunkt kan yde tilstrækkelig beskyttelse af EUCI til og med en nærmere bestemt klassifikationsgrad, og om, at dens medarbejdere, der skal have adgang til EUCI, er blevet behørigt sikkerhedsgodkendt og er gjort bekendt med de relevante sikkerhedskrav, der skal opfyldes med henblik på adgang til og beskyttelse af EUCI.

»forvaltning af klassificerede informationer«: se artikel 9, stk. 1.

»FSFP-operation«: en militær eller civil krisestyringsoperation i henhold til afsnit V, kapitel 2, i traktaten om Den Europæiske Union.

»fysisk sikkerhed«: se artikel 8, stk. 1.

»håndtering af EUCI«: alle de foranstaltninger, som EUCI kan underkastes i hele deres livscyklus. Dette omfatter udarbejdelse, behandling, transport, nedklassificering, afklassificering og destruktion. I forbindelse med CIS omfatter det også indsamling, visning, transmission og opbevaring.

»industrisikkerhed«: se artikel 11, stk. 1.

»industrivirksomhed eller anden enhed«: en enhed, der er involveret i levering af varer, udførelse af arbejder eller levering af tjenesteydelser; det kan være en enhed inden for industri, handel, tjenesteydelser, videnskab, forskning, uddannelse eller udvikling eller en selvstændig erhvervsdrivende.

»informationssikring«: se artikel 10, stk. 1.

»klassificeret kontrakt«: en kontrakt, som GSR indgår med en kontrahent om levering af varer, udførelse af arbejder eller levering af tjenesteydelser, såfremt kontraktens opfyldelse kræver eller indebærer adgang til eller udarbejdelse af EUCI.

»klassificeret underkontrakt«: en kontrakt, som en GSR-kontrahent indgår med en anden kontrahent (dvs. underkontrahenten) om levering af varer, udførelse af arbejder eller levering af tjenesteydelser, såfremt kontraktens opfyldelse kræver eller indebærer adgang til eller udarbejdelse af EUCI.

»klassifikationsvejledning« (SCG): et dokument, der beskriver de elementer af et program eller en kontrakt, som er klassificeret, med angivelse af de gældende klassifikationsgrader. SCG'en kan udvides i hele programmets eller kontraktens løbetid, og informationselementerne kan om- eller nedklassificeres. Når der findes en SCG, skal den indgå i SAL.

»kommunikations- og informationssystem« (CIS): se artikel 10, stk. 2.

»kontrahent«: en enkeltperson eller en retlig enhed, der har rets- og handleevne til at indgå kontrakter.

»kryptografisk (krypto)materiale«: kryptografiske algoritmer, kryptografiske hardware- og softwaremoduler samt produkter, der omfatter implementeringsdetaljer og tilhørende dokumentation og nøglingsmateriale.

»materiale«: ethvert dokument eller enhver maskine eller ethvert udstyr, der enten er fremstillet eller er ved at blive fremstillet.

»nedklassificering«: nedsættelse til en lavere klassifikationsgrad.

»personelsikkerhed«: se artikel 7, stk. 1.

»personelsikkerhedsgodkendelse« (PSC): en eller begge af følgende:

— »EU-personelsikkerhedsgodkendelse« (EU-PSC) med henblik på adgang til EUCI: en autorisation, der gives af GSR's ansættelsesmyndighed i overensstemmelse med denne afgørelse på baggrund af en sikkerhedsundersøgelse udført af en medlemsstats kompetente myndigheder, hvorved det attesteres, at vedkommende person kan få adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato, såfremt den pågældendes need-to-know-status er blevet fastslået; den pågældende person betegnes som »sikkerhedsgodkendt«.

— »national personelsikkerhedsgodkendelse« (national PSC) med henblik på adgang til EUCI: en erklæring fra en medlemsstats kompetente myndighed på baggrund af en sikkerhedsundersøgelse udført af en medlemsstats kompetente myndigheder, hvorved det attesteres, at vedkommende person kan få adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato, såfremt den pågældendes need-to-know-status er blevet fastslået; den pågældende person betegnes som »sikkerhedsgodkendt«.

»program-/projektsikkerhedsinstruktion« (PSI): en liste over sikkerhedsprocedurer, der anvendes i forbindelse med et bestemt program/projekt for at standardisere sikkerhedsprocedurerne. Den kan revideres i hele programmets/projektets løbetid.

»registrering«: se bilag III, punkt 18.

»residualrisiko«: den risiko, der fortsat eksisterer, efter at der er gennemført sikkerhedsforanstaltninger, idet ikke alle trusler imødegås, og ikke alle sårbarheder kan fjernes.

»risiko«: muligheden for, at en given trussel vil udnytte indre og ydre sårbarheder i en organisation eller i nogen af de systemer, det benytter, og derved skade organisationen og dets materielle eller immaterielle aktiver. Den måles som en kombination af sandsynligheden for, at trusler indtræffer, og deres virkning.

— »risikoaccept«: beslutningen om at acceptere, at der fortsat findes en residualrisiko efter risikobehandlingen

— »risikovurdering«: identifikation af trusler og sårbarheder og udførelse af den dertil knyttede risikoanalyse, dvs. analyse af sandsynlighed og virkning

— »risikokommunikation«: udvikling af bevidstheden om risici blandt CIS-brugere, underretning af godkendelsesmyndigheder om sådanne risici og indberetning af dem til driftsmyndigheder

— »risikobehandling«: at afbøde, fjerne, reducere (gennem en passende kombination af tekniske, fysiske, organisatoriske eller proceduremæssige foranstaltninger), flytte eller overvåge risikoen.

»sammenkobling«: se bilag IV, punkt 31.

»sikkerhedsmæssig driftsform«: fastlæggelse af de betingelser, hvorpå et CIS fungerer, baseret på klassifikationen af de informationer, der håndteres, og dets brugeres sikkerhedsgodkendelsesniveau, formelle adgangsgodkendelser og need-to-know-status. Der findes fire driftsformer for håndtering og transmission af klassificerede informationer: dedikeret, system-high, compartmented og multilevel

— »dedikeret«: en driftsform, hvor alle personer med adgang til CIS'et er godkendt til den højeste klassifikationsgrad for de informationer, der håndteres i CIS'et, og har en generel need-to-know-status for samtlige informationer, der håndteres i CIS'et

— »system-high«: en driftsform, hvor alle personer med adgang til CIS'et er godkendt til den højeste klassifikationsgrad for de informationer, der håndteres i CIS'et, men ikke alle personer med adgang til CIS'et har en generel need-to-know-status for de informationer, der håndteres i CIS'et; godkendelse af adgang til informationer kan gives af en person

— »compartmented«: en driftsform, hvor alle personer med adgang til CIS'et er godkendt til den højeste klassifikationsgrad for de informationer, der håndteres i CIS'et, men ikke alle personer med adgang til CIS'et har en formel autorisation til at have adgang til samtlige informationer, der håndteres i CIS'et; en formel autorisation indebærer en formel central styring af adgangskontrollen til forskel fra en persons mulighed for at give adgang

— »multilevel«: en driftsform, hvor ikke alle personer med adgang til CIS'et er godkendt til den højeste klassifikationsgrad for de informationer, der håndteres i CIS'et, og ikke alle personer med adgang til CIS'et har en generel need-to-know-status for de informationer, der håndteres i CIS'et.

»sikkerhedsrisikostyringsproces«: hele processen med at identificere, kontrollere og minimere usikre begivenheder, der kan påvirke sikkerheden i en organisation eller i de systemer, den anvender. Det omfatter samtlige risikorelaterede aktiviteter, herunder vurdering, behandling, accept og kommunikation.

»sikkerhedsundersøgelse«: de undersøgelser, som den kompetente myndighed i en medlemsstat foretager i overensstemmelse med denne stats nationale love og bestemmelser med henblik på at kunne konkludere, at der ikke er konstateret negative forhold, som kunne forhindre en person i at få en national PSC eller en EU-PSC med henblik på adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere).

»særlige sikkerhedsbetingelser« (SAL): et sæt særlige kontraktlige betingelser udstedt af den kontraherende myndighed, som er en integrerende del af en klassificeret kontrakt, der indebærer adgang til eller udarbejdelse af EUCI, og som fastlægger sikkerhedskravene eller de elementer i kontrakten, der kræver sikkerhedsbeskyttelse.

»sårbarhed«: en svaghed af enhver art, som kan udnyttes af en eller flere trusler. En sårbarhed kan være en forsømmelse eller vedrøre en svaghed i kontrolforanstaltninger med hensyn til effektivitet, omfang eller sammenhæng og være af teknisk, proceduremæssig, fysisk, organisatorisk eller operativ karakter.

»Tempest«: efterforskning, undersøgelse og kontrol af kompromitterende elektromagnetiske emissioner og foranstaltninger til at fjerne dem.

»trussel«: en potentiel årsag til en uønsket hændelse, der kan føre til skade på en organisation eller de systemer, den anvender; sådanne trusler kan være uagtsomme eller forsætlige (ondsindede) og karakteriseres ved trusselselementer, potentielle mål og angrebsmetoder.

»udpeget sikkerhedsmyndighed« (DSA): en myndighed, der med referat til en medlemsstats nationale sikkerhedsmyndighed (NSA) er ansvarlig for formidling til industrivirksomheder eller andre enheder af den nationale politik med hensyn til alle spørgsmål vedrørende industrisikkerhed og for opstilling af retningslinjer og ydelse af bistand i forbindelse med denne politiks gennemførelse. DSA'ens funktion kan varetages af NSA'en eller af en hvilken som helst anden kompetent myndighed.

»udsteder«: en EU-institution eller et EU-agentur eller -organ, en medlemsstat, et tredjeland eller en international organisation, under hvis myndighed klassificerede informationer er blevet udarbejdet og/eller bragt ind i EU's strukturer.

Tillæg B

SAMMENLIGNENDE OVERSIGT OVER SIKKERHEDSKLASSIFIKATIONER

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgien	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	jf. fodnote ([1])
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Den Tjekkiske Republik	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	STRENG GEHEIM	GEHEIM	VS ([2]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irland	Top Secret	Secret	Confidential	Restricted
Grækenland	Άκρως Απόρρητο Fork.: ΑΑΠ	Απόρρητο Fork.: (ΑΠ)	Εμπιστευτικό Fork.: (ΕΜ)	Περιορισμένης Χρήσης Fork.: (ΠΧ)
Spanien	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankrig	Très Secret Défense	Secret Défense	Confidentiel Défense	jf. fodnote ([3])
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Cypern	Άκρως Απόρρητο Fork.: (ΑΑΠ)	Απόρρητο Fork.: (ΑΠ)	Εμπιστευτικό Fork.: (ΕΜ)	Περιορισμένης Χρήσης Fork.: (ΠΧ)
Letland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungarn	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederlandene	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Østrig	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Rumænien	Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovenien	Strogo tajno	Tajno	Zaupno	Interno
Slovakiet	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sverige ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Det Forenede Kongerige	Top Secret	Secret	Confidential	Restricted

([1]) Diffusion Restreinte/Beperkte Verspreiding er ikke en sikkerhedsklassifikation i Belgien. Belgien håndterer og beskytter informationer, der er mærket »RESTREINT UE/EU RESTRICTED«, på en måde, der mindst svarer til de standarder og procedurer, som er beskrevet i sikkerhedsreglerne for Rådet for Den Europæiske Union.

([2]) Tyskland: VS = Verschlusssache.

([3]) Frankrig anvender ikke klassifikationsgraden »RESTREINT« i sit nationale system. Frankrig håndterer og beskytter informationer, der er mærket »RESTREINT UE/EU RESTRICTED«, på en måde, der mindst svarer til de standarder og procedurer, som er beskrevet i sikkerhedsreglerne for Rådet for Den Europæiske Union.

([4]) Sverige: klassifikationsmærkningerne i øverste række anvendes af forsvarsmyndighederne og mærkningerne i nederste række af andre myndigheder.

Tillæg C

FORTEGNELSE OVER DE NATIONALE SIKKERHEDSMYNDIGHEDER (NSA'er)

BELGIEN
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tlf.: sekretariatet: + 32 2501 45 42
Fax + 32 2501 45 96
E-mail: nvo-ans@diplobel.fed.be

BULGARIEN
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tlf: + 359 29215911
Fax + 359 29873750
E-mail: dksi@government.bg
Webside: www.dksi.bg

DEN TJEKKISKE REPUBLIK
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tlf: + 420 257283335
Fax + 420257283110
E-mail: czech.nsa@nbu.cz
Webside: www.nbu.cz

IRLAND
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Ireland

Tlf: + 353 14780822
Fax + 353 14082959

GRÆKENLAND
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: + 30 21065 6279
+ 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens

Tlf: + 30 2106572045
+ 30 2106572009
Fax + 30 2106536279
+ 30 2106577612

DANMARK
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tlf: + 45 33148888
Fax + 45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tlf: + 45 33325566
Fax + 45/33/93 13 20

TYSKLAND
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin

Tlf: + 49 30186810
Fax + 49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTLAND
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tlf: +372 7170113, +372 7170117
Fax +372 7170213
E-mail: nsa@kmin.ee

SPANIEN
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tlf: + 34 913725000
Fax + 34 913725808
E-mail: nsa-sp@areatec.com

FRANKRIG
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tlf: + 33 171758177
Fax + 33 171758200

ITALIEN
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tlf: + 39 0661174266
Fax + 39 064885273

LETLAND
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga

Tlf: +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

CYPERN
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43,
+ 357 22807764
Τηλεομοιότυπο: + 357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tlf: + 357 2280 7569, + 357 228076 43,
+357 22807764
Fax: + 357 22302351
E-mail: cynsa@mod.gov.cy

LITAUEN
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Tlf: + 370 52663201,
+370 52663202
Fax + 370 52663200
E-mail: nsa@vsd.lt

LUXEMBOURG
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tlf: + 352 24782210 central
+ 352 24782253 direkte
Fax + 352 247822 43

NEDERLANDENE
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tlf: + 31 703204400
Fax + 31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tlf: + 31 703187060
Fax + 31 703187522

UNGARN
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tlf: + 361 3469652
Fax + 361 3469658
E-mail: nbf@nbf.hu
Webside: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
Valletta

Tlf: + 356 21249844
Fax + 356 25695321

ØSTRIG
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tlf: + 43 1531152594
Fax + 43 1531152615
E-mail: ISK@bka.gv.at

POLEN
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa

Tlf: + 48 225857360
Fax + 48 225858509
E-mail: nsa@abw.gov.pl
Webside: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Oczki 1
02-007 Warszawa

Tlf: + 48 226841247
Fax + 48 226841076
E-mail: skw@skw.gov.pl

RUMÆNIEN
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
12275 Bucharest

Tlf: + 40 212245830
Fax + 40 212240714
E-mail: nsa.romania@nsa.ro
Webside: www.orniss.ro

PORTUGAL
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tlf: +351 213031710
Fax +351 213031711

SLOVENIEN
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
Sl-1000 Ljubljana

Tlf: + 386 14781390
Fax + 386 14781399

SLOVAKIET
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tlf: + 421 2686923 14
Fax + 421 2/63824005
Webside: www.nbusr.sk

SVERIGE
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm

Tlf: + 46 84051000
Fax + 46 8/7231176
E-mail: ud-nsa@foreign.ministry.se

FINLAND
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Tlf 1: + 358 916056487
Tlf 2: + 358 916056484
Fax + 358 916055140
E-mail: NSA@formin.fi

UNITED KINGDOM
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Tlf 1: + 44 2072765649
Tlf 2: + 44 2072765497
Fax + 44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendiks D

LISTE OVER FORKORTELSER

Akronym	Betydning
AQUA	Kvalificeret evalueringsmyndighed (Appropriately Qualified Authority)
BPS	Grænsebeskyttelsestjenester (Boundary Protection Services)
CAA	Kryptogodkendelsesmyndighed (Crypto Approval Authority)
CCTV	Intern tv-overvågning (Closed Circuit Television)
CDA	Kryptodistributionsmyndighed (Crypto Distribution Authority)
CIS	Kommunikations- og informationssystemer, der håndterer EUCI (Communication and Information Systems handling EUCI)
COREPER	De Faste Repræsentanters Komité (Committee of Permanent Representatives)
DSA	Udpeget sikkerhedsmyndighed (Designated Security Authority)
ECSD	Kommissionens Direktorat for Sikkerhed (European Commission Security Directorate)
EUCI	EU's klassificerede informationer (EU Classified Information)
EUSR	EU's særlige repræsentant (EU Special Representative)
FSC	Facilitetssikkerhedsgodkendelse (Facility Security Clearance)
FSFP	Fælles sikkerheds- og forsvarspolitik
FUSP	Fælles udenrigs- og sikkerhedspolitik (Common Foreign and Security Policy)
GSR	Generalsekretariatet for Rådet
IA	Informationssikring (Information Assurance)
IAA	IA-myndighed (Information Assurance Authority)
IDS	System til afsløring af indtrængen (Intrusion Detection System)
IT	Informationsteknologi (Information Technology)
NSA	National sikkerhedsmyndighed (National Security Authority)
PSC	Personelsikkerhedsgodkendelse (Personnel Security Clearance)
PSCC	Certifikat for personelsikkerhedsgodkendelse (Personnel Security Clearance Certificate)
PSI	Program-/projektsikkerhedsinstruktion (Programme/Project Security Instructions)
SAA	Sikkerhedsakkrediteringsmyndighed (Security Accreditation Authority)
SAB	Sikkerhedsakkrediteringsudvalg (Security Accreditation Board)
SAL	Særlige sikkerhedsbetingelser (Security Aspects Letter)
SCG	Klassifikationsvejledning (Security Classification Guide)
SecOPs	Operationelle sikkerhedsprocedurer (Security Operating Procedures)
SSRS	Systemspecifikke sikkerhedskrav (System-Specific Security Requirement Statement)
TA	Tempestmyndighed (TEMPEST Authority)