

KOMMISSIONENS AFGØRELSE (EU, Euratom) 2015/444
af 13. marts 2015
om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 249,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 106,

under henvisning til protokol nr. 7 vedrørende Den Europæiske Unions privilegier og immuniteter, særlig artikel 18, og

ud fra følgende betragtninger:

- (1) Kommissionens regler for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUCI) bør revideres og ajourføres under hensyntagen til den institutionelle, organisatoriske, operationelle og teknologiske udvikling.
- (2) Europa-Kommissionen har indgået aftaler om sikkerhedsanliggender for sine vigtigste lokaliteter med den belgiske regering, den luxembourgske regering og den italienske regering ⁽¹⁾.
- (3) Kommissionen, Rådets og Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten) er fast besluttet på at anvende ækvivalente sikkerhedsstandarder for beskyttelse af EUCI.
- (4) Det er vigtigt, 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.
- (5) Risici for 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 i overensstemmelse med begrebet dybdeforsvar. Effekten af sådanne foranstaltninger skal løbende evalueres.
- (6) I Kommissionen forstås ved fysisk sikkerhed med henblik på at beskytte klassificerede informationer anvendelse af fysiske og tekniske beskyttelsesforanstaltninger for at forhindre uautoriseret adgang til EUCI.
- (7) Ved forvaltning af EUCI forstås anvendelse af administrative foranstaltninger til kontrol af EUCI i hele deres livscyklus med henblik på at supplere foranstaltningerne i kapitel 2, 3 og 5 i denne afgørelse og derved bidrage til at afværge, afsløre og udbedre forsætlig eller uagtsom kompromittering eller tab af sådanne informationer. Sådanne foranstaltninger omfatter bl.a. udarbejdelse, lagring, registrering, kopiering, oversættelse, nedklassificering, afklassificering, transport og destruktion af EUCI, og de supplerer Kommissionens generelle regler om dokumentforvaltning (afgørelse 2002/47/EF, EKSF, Euratom ⁽²⁾ og 2004/563/EF, Euratom ⁽³⁾).

⁽¹⁾ Jf. »Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité« af 31. december 2004, »Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois« af 20. januar 2007 og »Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale« af 22. juli 1959.

⁽²⁾ Kommissionens afgørelse 2002/47/EF, EKSF, Euratom af 23. januar 2002 om ændring af dens forretningsorden (EFT L 21 af 24.1.2002, s. 23).

⁽³⁾ Kommissionens afgørelse 2004/563/EF, Euratom af 7. juli 2004 om ændring af dens forretningsorden (EUT L 251 af 27.7.2004, s. 9).

- (8) Bestemmelserne i denne afgørelse gælder med forbehold af:
- a) forordning (Euratom) nr. 3 ⁽¹⁾
 - b) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 ⁽²⁾
 - c) Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 ⁽³⁾
 - d) Rådets forordning (EØF, Euratom) nr. 354/83 ⁽⁴⁾ —

VEDTAGET DENNE AFGØRELSE:

KAPITEL 1

GRUNDLÆGGENDE PRINCIPPER OG MINIMUMSSTANDARDE

Artikel 1

Definitioner

I denne afgørelse forstås ved:

- 1) »kommissionstjenestegren«: et generaldirektorat eller en tjeneste i Kommissionen eller et kommissionsmedlems kabinet
- 2) »kryptografisk (krypto)materiale«: algoritmer, kryptografiske hardware- og softwaremoduler samt produkter, der omfatter implementeringsdetaljer og tilhørende dokumentation og nøglingsmateriale
- 3) »afklassificering«: fjernelse af enhver sikkerhedsklassifikation
- 4) »dybdeforsvar«: anvendelse af en række sikkerhedsforanstaltninger, der er organiseret som flere lag af forsvarsmekanismer
- 5) »dokument«: registrerede informationer uanset deres fysiske form eller karakteristika
- 6) »nedklassificering«: nedsættelse til en lavere klassifikationsgrad
- 7) »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 kommunikations- og informationssystemer (CIS) omfatter det også indsamling, visning, transmission og opbevaring
- 8) »den, der er i besiddelse af«: en behørigt autoriseret person med en fastslået need-to-know, der er i besiddelse af EUCI og derfor er ansvarlig for at beskytte dem
- 9) »gennemførelsesbestemmelser«: alle regelsæt eller sikkerhedsmeddelelser, der er vedtaget i henhold til kapitel 5 i Kommissionens afgørelse (EU, Euratom) 2015/443 ⁽⁵⁾
- 10) »materiale«: ethvert medium, enhver databærer, enhver maskine eller ethvert udstyr, der enten er fremstillet eller er ved at blive fremstillet
- 11) »udsteder«: en EU-institution eller et EU-organ eller -agentur, en medlemsstat, et tredjeland eller en international organisation, under hvis myndighed klassificerede informationer er blevet udarbejdet og/eller bragt ind i Unionens strukturer
- 12) »lokaliteter«: Kommissionens faste ejendom eller tilsvarende ejendom og besiddelser

⁽¹⁾ Forordning (Euratom) nr. 3 af 31. juli 1958 om anvendelse af artikel 24 i traktaten om oprettelse af Det europæiske Atomenergifællesskab (EFT L 17 af 6.10.1958, s. 406/58).

⁽²⁾ Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).

⁽³⁾ Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

⁽⁴⁾ Rådets forordning (EØF, Euratom) nr. 354/83 af 1. februar 1983 om åbning for offentligheden af de historiske arkiver for Det europæiske økonomiske Fællesskab og Det europæiske Atomenergifællesskab (EFT L 43 af 15.2.1983, s. 1).

⁽⁵⁾ Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhed i Kommissionen (se side 41 i denne EUT).

- 13) »sikkerhedsrisikostyringsproces«: hele processen med at identificere, kontrollere og minimere usikre begivenheder, der kan påvirke sikkerheden i en organisation eller i de systemer, den anvender. Dette omfatter samtlige risikorelaterede aktiviteter, herunder vurdering, behandling, accept og kommunikation
- 14) »personalevedtægten«: vedtægten for tjenestemænd i Den Europæiske Union og ansættelsesvilkårene for Den Europæiske Unions øvrige ansatte som fastlagt i Rådets forordning (EØF, Euratom, EKSF) nr. 259/68 ⁽¹⁾
- 15) »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
- 16) »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 deres effektivitet, omfang eller sammenhæng og være af teknisk, proceduremæssig, fysisk, organisatorisk eller operativ karakter.

Artikel 2

Genstand og anvendelsesområde

1. Denne afgørelse fastlægger grundprincipperne og minimumsstandarderne for sikkerhedsbeskyttelse af EUCI.
2. Denne afgørelse finder anvendelse på alle kommissionstjenestegrene og på alle Kommissionens lokaliteter.
3. Uanset specifikke angivelser vedrørende særlige personalegrupper skal denne afgørelse gælde for medlemmer af Kommissionen, for kommissionsansatte, der er omfattet af vedtægten for tjenestemænd og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber, for udstationerede nationale eksperter i Kommissionen, for tjenesteudbydere og deres personale, for praktikanter og for alle med adgang til Kommissionens bygninger eller andre aktiver eller til informationer, der håndteres af Kommissionen.
4. Bestemmelserne i denne afgørelse berører ikke afgørelse 2002/47/EF, EKSF, Euratom og afgørelse 2004/563/EF, Euratom.

Artikel 3

Definition af EUCI, sikkerhedsklassifikationer og mærkninger

1. Ved »EU-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, som ikke er klassifikationsmærkninger, men som skal angive de berørte aktivitetsområder, identificere udstederen, begrænse distributionen eller anvendelsen eller angive mulighederne for videregivelse.

⁽¹⁾ Rådets forordning (EØF, Euratom, EKSF) nr. 259/68 af 29. februar 1968 om vedtægten for tjenestemænd i De Europæiske Fællesskaber og om ansættelsesvilkårene for de øvrige ansatte i disse Fællesskaber samt om særlige midlertidige foranstaltninger for tjenestemænd i Kommissionen (Vilkårene for de øvrige ansatte) (EFT L 56 af 4.3.1968, s. 1).

*Artikel 4***Klassifikationsstyring**

1. Ethvert medlem af Kommissionen eller af en kommissionstjenestegren sikrer, at EUCI, som vedkommende udarbejder, klassificeres korrekt, tydeligt identificeres som EUCI og kun bevarer klassifikationsgraden, så længe det er nødvendigt.
2. Med forbehold af artikel 26 må EUCI ikke nedklassificeres eller afklassificeres, og ingen af de klassifikationsmærkninger, der er anført i artikel 3, stk. 2, må ændres eller fjernes uden forudgående skriftligt samtykke fra udstederen.
3. Der vedtages om nødvendigt gennemførelsesbestemmelser om håndtering af EUCI, herunder en praktisk klassifikationsvejledning, jf. artikel 60.

*Artikel 5***Beskyttelse af klassificerede informationer**

1. EUCI beskyttes i overensstemmelse med denne afgørelse og dens gennemførelsesbestemmelser.
2. Den, der er i besiddelse af EUCI, er ansvarlig for beskyttelsen heraf i overensstemmelse med denne afgørelse og dens gennemførelsesbestemmelser, jf. reglerne i kapitel 4.
3. Hvis medlemsstaterne bringer klassificerede informationer med en national klassifikationsmærkning ind i Kommissionens strukturer eller netværk, beskytter Kommissionen disse informationer i overensstemmelse med de krav, der gælder for EUCI af en tilsvarende grad, jf. den sammenlignende oversigt over sikkerhedsklassifikationer i bilag I.
4. En samlet mængde af EUCI kan berettige til en sikkerhedsbeskyttelse af en grad, der svarer til en højere klassifikation end den, der gælder for de enkelte dele.

*Artikel 6***Sikkerhedsrisikostyring**

1. Sikkerhedsforanstaltninger til beskyttelse af EUCI i hele deres livscyklus skal især svare til EUCI's sikkerhedsklassifikation, formen og mængden af informationer eller materiale, 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.
2. 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.
3. Alle tjenesters kontinuitetsplaner skal omfatte forebyggende og genoprettende foranstaltninger med henblik på at minimere følgerne af større nedbrud eller hændelser vedrørende håndtering og opbevaring af EUCI.

*Artikel 7***Gennemførelse af denne afgørelse**

1. Der vedtages om nødvendigt gennemførelsesbestemmelser om håndtering af EUCI, herunder en praktisk klassifikationsvejledning, jf. artikel 60.
2. Kommissionstjenestegrenene træffer alle fornødne foranstaltninger, der henhører under deres ansvarsområde, til at sikre, at denne afgørelse og de relevante gennemførelsesbestemmelser anvendes i forbindelse med håndtering eller lagring af EUCI eller andre klassificerede informationer.
3. De sikkerhedsforanstaltninger, der træffes i forbindelse med gennemførelsen af denne afgørelse, skal være i overensstemmelse med principperne for sikkerhed i Kommissionen, jf. artikel 3 i afgørelse (EU, Euratom) 2015/443.

4. Generaldirektøren for menneskelige ressourcer og sikkerhed opretter Kommissionens sikkerhedsmyndighed i Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed. Kommissionens sikkerhedsmyndighed varetager de opgaver, som tildeles den ved denne afgørelse og de dertil hørende gennemførelsesbestemmelser.

5. I hver af kommissionstjenestegrenene har den lokale sikkerhedsansvarlige (LSO), jf. artikel 20 i afgørelse (EU, Euratom) 2015/443, i tæt samarbejde med Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed følgende overordnede ansvar for beskyttelse af EUCI i overensstemmelse med denne afgørelse og skal:

- a) forvalte anmodninger om sikkerhedsgodkendelse af personale
- b) bidrage til sikkerhedsuddannelse og bevidsthedsorientering
- c) føre tilsyn med tjenestegrenens arkivansvarlige (RCO)
- d) indberette brud på sikkerheden og kompromittering af EUCI
- e) opbevare reservenøgler samt en skriftlig fortegnelse over alle de koder, der kan anvendes
- f) varetage andre opgaver, som vedrører beskyttelsen af EUCI eller er fastlagt i gennemførelsesbestemmelserne.

Artikel 8

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 og dens gennemførelsesbestemmelser.
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 Kommissionens sikkerhedsmyndighed.
4. Hvis det konstateres, eller hvis der er rimelig grund til at formode, at EUCI er kompromitteret eller bortkommet, skal der foretages en sikkerhedsundersøgelse i overensstemmelse med artikel 13 i afgørelse (EU, Euratom) 2015/443.
5. Der skal træffes alle passende foranstaltninger til 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 Unionens eller medlemsstaternes interesser
 - d) træffe passende foranstaltninger til at forebygge en gentagelse og
 - e) underrette de relevante myndigheder om de foranstaltninger, der er truffet.
6. Enhver, der er ansvarlig for brud på sikkerhedsreglerne i denne afgørelse, kan pålægges disciplinære foranstaltninger i overensstemmelse med vedtægten. Enhver, der er ansvarlig for kompromittering eller bortkomst af EUCI, pålægges disciplinære foranstaltninger og/eller retsforfølgelse i overensstemmelse med gældende love, regler og bestemmelser.

KAPITEL 2

PERSONELSIKKERHED

Artikel 9

Definitioner

I dette kapitel forstås ved:

- 1) »autorisation til at få adgang til EUCI«: en afgørelse truffet af Kommissionens sikkerhedsmyndighed på grundlag af en sikkerhedskonklusion fra en kompetent myndighed i en medlemsstat om, at en tjenestemand i Kommissionen, en anden ansat eller udstationeret national ekspert, såfremt den pågældendes need-to-know er fastslået, og vedkommende er blevet behørigt orienteret om sit ansvar, kan tildeles adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato; den pågældende person betegnes som »sikkerhedsautoriseret«.

- 2) »personelsikkerhedsautorisation«: anvendelse af foranstaltninger for at sikre, at adgang til EUCI kun gives til personer, som:
 - a) har need-to-know
 - b) er sikkerhedsautoriseret til den relevante klassifikationsgrad, når det er nødvendigt, og
 - c) er blevet orienteret om deres ansvar.
- 3) »personelsikkerhedsgodkendelse« (PSC): en erklæring fra en medlemsstats kompetente myndighed på baggrund af en sikkerhedsundersøgelse udført af en medlemsstats kompetente myndigheder, hvorved det attesteres, at en person, forudsat at vedkommendes need-to-know er fastslået, og at vedkommende er blevet behørigt orienteret om sit ansvar, kan få adgang til EUCI op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere) indtil en bestemt dato
- 4) »certifikat for personelsikkerhedsgodkendelse« (PSCC): et certifikat udstedt af en kompetent myndighed, som fastslår, at en person har en gyldig sikkerhedsgodkendelse eller sikkerhedsautorisation fra Kommissionens sikkerhedsmyndighed, som viser den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), den pågældende sikkerhedsgodkendelses eller sikkerhedsautorisations gyldighedsperiode og certifikatets udløbsdato.
- 5) »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 nå til den konklusion, at der ikke er konstateret negative forhold, som kunne forhindre en person i at få en sikkerhedsgodkendelse op til en bestemt klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere).

Artikel 10

Grundprincipper

1. En person kan kun få adgang til klassificerede informationer, efter at:
 - 1) vedkommendes need-to-know er fastslået
 - 2) vedkommende er blevet orienteret om regler og procedurer for sikkerhedsbeskyttelse af EUCI og de relevante sikkerhedsstandarder og sikkerhedsretningslinjer og har anerkendt sit ansvar med hensyn til beskyttelse af sådan informationer
 - 3) vedkommende i forbindelse med informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, er blevet sikkerhedsautoriseret til den relevante klassifikationsgrad eller på anden måde er behørigt autoriseret i kraft af sine funktioner i overensstemmelse med nationale love og bestemmelser.
2. Alle personer, hvis opgaver kan forudsætte adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal være sikkerhedsautoriseret til den relevante klassifikationsgrad, inden de kan få adgang til sådanne EUCI. Den pågældende skal skriftligt give sit samtykke til at blive underkastet proceduren for personelsikkerhedsgodkendelse. Undladelse heraf betyder, at vedkommende ikke kan tildeles en stilling, en funktion eller en opgave, som involverer adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere.
3. 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.
4. For at kunne fastslå, om en person er loyal, troværdig og pålidelig, således at vedkommende kan blive sikkerhedsgodkendt til at få adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, foretager de kompetente myndigheder i en medlemsstat en sikkerhedsundersøgelse i overensstemmelse med denne stats nationale love og bestemmelser.
5. Kommissionens sikkerhedsmyndighed er eneansvarlig for forbindelserne til de nationale sikkerhedsmyndigheder (NSA) eller andre kompetente myndigheder i forbindelse med alle spørgsmål om sikkerhedsgodkendelse. Al kontakt mellem Kommissionens tjenester og deres ansatte og NSA'er og andre kompetente myndigheder skal foregå gennem Kommissionens sikkerhedsmyndighed.

Artikel 11

Procedure for sikkerhedsautorisation

1. Alle generaldirektører eller chefer for en tjeneste i Kommissionen skal udpege de stillinger i deres tjenestegren, som indebærer, at den, der bestrider stillingen, skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, for at kunne udføre sit arbejde, og som derfor skal sikkerhedsautoriseres.

2. Så snart det konstateres, at en person vil blive udnævnt til en stilling, der kræver adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, underretter LSO i den pågældende kommissionstjenestegren Kommissionens sikkerhedsmyndighed, som sender vedkommende det spørgeskema vedrørende sikkerhedsgodkendelse, der er udstedt af den nationale sikkerhedsmyndighed i den medlemsstat, hvorfra personen er blevet ansat i de europæiske institutioner. Personen skal skriftligt give sit samtykke til at blive underkastet sikkerhedsgodkendelsesproceduren og skal returnere det udfyldte spørgeskema hurtigst muligt til Kommissionens sikkerhedsmyndighed.
3. Kommissionens sikkerhedsmyndighed videregiver det udfyldte spørgeskema vedrørende sikkerhedsgodkendelse til NSA'en i den medlemsstat, hvorfra personen er blevet ansat i de europæiske institutioner, med anmodning om, at der foretages en sikkerhedsundersøgelse for den EUCI-klassifikationsgrad, hvortil personen har brug for adgang.
4. Hvis Kommissionens sikkerhedsmyndighed får kendskab til oplysninger, der er relevante for en sikkerhedsundersøgelse, om en person, der har ansøgt om sikkerhedsgodkendelse, underretter Kommissionens sikkerhedsmyndighed den relevante nationale sikkerhedsmyndighed herom i overensstemmelse med de relevante regler og forskrifter.
5. Når sikkerhedsundersøgelsen er gennemført, og hurtigst muligt efter at den relevante NSA har meddelt sin overordnede vurdering af resultaterne af sikkerhedsundersøgelsen:
 - a) kan Kommissionens sikkerhedsmyndighed give den pågældende person autorisation til at få adgang til EUCI og tillade adgang til EUCI op til den relevante klassifikationsgrad indtil en bestemt dato, dog højst i fem år, hvis sikkerhedsundersøgelsen fører til den konklusion, at der ikke er konstateret negative forhold, som kan rejse tvivl om personens loyalitet, troværdighed og pålidelighed
 - b) skal Kommissionens sikkerhedsmyndighed, hvis sikkerhedsundersøgelsen ikke fører til denne konklusion, underrette den pågældende person, der kan anmode om at blive hørt af Kommissionens sikkerhedsmyndighed, som kan anmode den relevante NSA om eventuelle nærmere oplysninger, som denne kan give i overensstemmelse med de nationale love og bestemmelser. Såfremt resultatet af sikkerhedsundersøgelsen bekræftes, tildeles der ikke autorisation til at få adgang til EUCI.
6. Sikkerhedsundersøgelsen samt de opnåede resultater er underlagt de relevante love og bestemmelser, som er gældende i den pågældende medlemsstat, herunder bestemmelser om klageadgang. Klager over afgørelser truffet af Kommissionens sikkerhedsmyndighed indgives i overensstemmelse med personalevedtægten.
7. Kommissionen accepterer en autorisation til at få adgang til EUCI, der er tildelt af en anden EU-institution eller et andet EU-organ eller -agentur, forudsat at den stadig er gyldig. Autorisationen skal omfatte alle de arbejdsopgaver, den pågældende person udfører i Kommissionen. Den EU-institution eller det EU-organ eller -agentur, hvor personen påbegynder sin ansættelse, giver den relevante NSA meddelelse om den nye arbejdsgiver.
8. Hvis en persons ansættelsesperiode ikke påbegyndes inden for 12 måneder efter meddelelsen af sikkerhedsundersøgelsens resultat til Kommissionens sikkerhedsmyndighed, eller hvis personens ansættelse afbrydes i en periode på 12 måneder, uden at der i samme periode sker ansættelse i Kommissionen eller i en anden EU-institution eller et andet EU-organ eller -agentur, eller i en medlemsstats nationale administration, skal Kommissionens sikkerhedsmyndighed meddele den relevante NSA dette forhold med henblik på at få bekræftet, at sikkerhedsgodkendelsen fortsat er gyldig og relevant.
9. Hvis Kommissionens sikkerhedsmyndighed får kendskab til oplysninger om, at en person, der er i besiddelse af en gyldig sikkerhedsautorisation, udgør en sikkerhedsrisiko, underretter sikkerhedsmyndigheden den relevante NSA herom i overensstemmelse med de relevante regler og bestemmelser.
10. Når en NSA underretter Kommissionens sikkerhedsmyndighed om, at den trækker en sikkerhedskonklusion tilbage, der er givet i overensstemmelse med stk. 5, litra a), vedrørende en person, der er i besiddelse af en gyldig autorisation til adgang til EUCI, kan Kommissionens sikkerhedsmyndighed anmode NSA'en om de nærmere oplysninger, som denne er i stand til at give i henhold til de nationale love og bestemmelser. Hvis den pågældende NSA bekræfter de negative oplysninger, inddrages sikkerhedsautorisationen, 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.
11. En afgørelse om at inddrage eller suspendere en autorisation til adgang til EUCI fra en person, der er omfattet af denne afgørelse, og, når det er relevant, grundene hertil skal meddeles den pågældende person, som kan anmode om at blive hørt af Kommissionens sikkerhedsmyndighed. Oplysninger, der videregives af en NSA, er underlagt den pågældende medlemsstats relevante love og bestemmelser. Klager over afgørelser, der træffes i denne forbindelse af Kommissionens sikkerhedsmyndighed, kan indgives i overensstemmelse med personalevedtægten.

12. Kommissionstjenestegrenene sikrer sig, at nationale eksperter, der udstationeres til en stilling, hvortil der kræves en sikkerhedsautorisation for at få adgang til EUCI, inden de påbegynder arbejdet, fremlægger en gyldig personelsikkerhedsgodkendelse (PSC) eller et gyldigt certifikat for personelsikkerhedsgodkendelse (PSCC) for Kommissionens sikkerhedsmyndighed, som på grundlag heraf tildeler en sikkerhedsautorisation til adgang til EUCI til en grad svarende til den, der er omhandlet i den nationale sikkerhedsgodkendelse, af en gyldighed, der højst svarer til varigheden af deres udstationering.

Adgang til EUCI for personer, der er autoriserede i kraft af deres funktioner

13. Medlemmer af Kommissionen, som har adgang til EUCI i kraft af deres funktioner på grundlag af traktaten, skal orienteres om deres sikkerhedsmæssige forpligtelser med hensyn til beskyttelse af EUCI.

Registre over sikkerhedsgodkendelser og sikkerhedsautorisationer

14. Registre over de sikkerhedsgodkendelser og autorisationer, der er tildelt med henblik på at give adgang til EUCI, føres af Kommissionens sikkerhedsmyndighed i overensstemmelse med denne afgørelse. Disse registre skal mindst indeholde den klassifikationsgrad for EUCI, som personen kan få adgang til, datoen for udstedelse af sikkerhedsgodkendelsen samt dens gyldighedsperiode.

15. Den kompetente sikkerhedsmyndighed kan udstede en PSCC med angivelse af den klassifikationsgrad for EUCI, som personen kan få adgang til (CONFIDENTIEL UE/EU CONFIDENTIAL eller højere), gyldighedsdatoen for den relevante autorisation til adgang til EUCI og certifikatets udløbsdato.

Fornyelse af sikkerhedsautorisationer

16. Har personen været i uafbrudt tjeneste i Europa-Kommissionen eller en anden europæisk institution, et EU-organ eller -agentur efter den første tildeling af en sikkerhedsautorisation, og har den pågældende fortsat behov for adgang til EUCI, skal sikkerhedsautorisationen til adgang til EUCI generelt tages op til revision med henblik på fornyelse hvert femte år fra datoen for meddelelsen af resultatet af den seneste sikkerhedsundersøgelse, som den bygger på.

17. Kommissionens sikkerhedsmyndighed kan forlænge gyldigheden af den gældende sikkerhedsautorisation i en periode på op til 12 måneder, hvis den ikke har modtaget negative oplysninger fra den relevante NSA eller en anden kompetent national myndighed inden for to måneder fra datoen for videresendelsen af anmodningen om fornyelse og det tilsvarende spørgeskema vedrørende sikkerhedsgodkendelse. Hvis den relevante NSA eller en anden kompetent national myndighed ikke inden udgangen af den 12-måneders periode har meddelt Kommissionens sikkerhedsmyndighed sin holdning, gives den pågældende person opgaver, som ikke kræver en sikkerhedsautorisation.

Artikel 12

Orientering om sikkerhedsautorisation

1. Efter at have deltaget i en orientering om sikkerhedsautorisation tilrettelagt af Kommissionens sikkerhedsmyndighed skal alle personer, som er blevet sikkerhedsautoriserede, skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og konsekvenserne af en eventuel kompromittering af EUCI. Kommissionens sikkerhedsmyndighed fører et register over sådanne skriftlige bekræftelser.

2. Alle personer, der er autoriseret til at få adgang til, eller som skal håndtere EUCI, skal indledningsvis gøres opmærksomme på og dernæst regelmæssigt orienteres om sikkerhedsrisici, og de skal øjeblikkelig indberette enhver henvendelse eller aktivitet, de finder mistænkelig eller usædvanlig, til Kommissionens sikkerhedsmyndighed.

3. 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.

Artikel 13

Midlertidige sikkerhedsautorisationer

1. Kommissionens sikkerhedsmyndighed kan i særlige tilfælde, 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 til undersøgelse af, at der ikke er konstateret negative oplysninger, give personer midlertidig autorisation til at få adgang til EUCI med henblik på en specifik opgave, jf. dog bestemmelserne om fornyelse af sikkerhedsgodkendelser. Sådanne midlertidige autorisationer til adgang til EUCI er gyldige i en periode på højst seks måneder og tillader ikke adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET.

2. Efter en orientering i overensstemmelse med artikel 12, stk. 1, skal alle personer, der har fået en midlertidig autorisation, skriftligt bekræfte, at de har forstået deres forpligtelser med hensyn til beskyttelse af EUCI og konsekvenserne af en eventuel kompromittering af EUCI. Kommissionens sikkerhedsmyndighed fører et register over sådanne skriftlige bekræftelser.

Artikel 14

Deltagelse i klassificerede møder afholdt af Kommissionen

1. De kommissionstjenestegrene, der har ansvar for at afholde møder, hvorpå der drøftes informationer klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal via deres LSO eller mødearrangøren i god tid underrette Kommissionens sikkerhedsmyndighed om mødedato, mødetidspunkt, mødested og mødedeltagere.

2. I overensstemmelse med artikel 11, stk. 13, må personer, der skal deltage i møder, der afholdes af Kommissionen, og hvorpå der drøftes informationer klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, først deltage, når deres status af sikkerhedsgodkendt eller sikkerhedsautoriseret er bekræftet. Der må ikke gives adgang til sådanne klassificerede møder for personer, for hvem Kommissionens sikkerhedsmyndighed ikke har set en PSCC eller andet bevis for sikkerhedsgodkendelse, eller for deltagere fra Kommissionen, som ikke er i besiddelse af en sikkerhedsautorisation.

3. Før tilrettelæggelsen af et klassificeret møde anmoder mødearrangøren eller LSO i den kommissionstjenestegren, som står for mødet, eksterne deltagere om at forelægge Kommissionens sikkerhedsmyndighed en PSCC eller det andet bevis på sikkerhedsgodkendelse. Kommissionens sikkerhedsmyndighed underretter LSO eller mødearrangøren om den PSCC eller det andet bevis for PSC, den har modtaget. Der kan eventuelt anvendes en konsolideret navneliste, som indeholder den relevante dokumentation for sikkerhedsgodkendelse.

4. Hvis Kommissionens sikkerhedsmyndighed af de kompetente myndigheder underrettes om, at en PSC er blevet trukket tilbage fra en person, hvis opgaver forudsætter deltagelse i møder afholdt af Kommissionen, skal sikkerhedsmyndigheden meddele dette til LSO i den kommissionstjenestegren, der er ansvarlig for at tilrettelægge mødet.

Artikel 15

Potentiel adgang til EUCI

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

KAPITEL 3

FYSISK SIKKERHED MED HENBLIK PÅ BESKYTTELSE AF KLASIFICEREDE INFORMATIONER

Artikel 16

Grundprincipper

1. De fysiske sikkerhedsforanstaltninger udformes med henblik på at forhindre, at en indtrænger skaffer sig hemmelig adgang eller tiltvinger sig adgang, at afværge, vanskeliggøre og afsløre uautoriserede handlinger samt at muliggøre personalemæssig adskillelse for så vidt angår adgang til EUCI på en need-to-know-basis. Sådanne foranstaltninger skal fastlægges på grundlag af en risikostyringsproces i overensstemmelse med denne afgørelse og dens gennemførelsesbestemmelser.

2. Navnlig de fysiske sikkerhedsforanstaltninger skal 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.

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. kapitel 5.
4. Områder, hvor EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, opbevares, skal etableres som sikrede områder i overensstemmelse med dette kapitel og godkendes af Kommissionens sikkerhedsakkrediteringsmyndighed.
5. Der må kun anvendes udstyr eller anordninger, der er godkendt af Kommissionens sikkerhedsmyndighed, til beskyttelse af EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere.

Artikel 17

Fysiske sikkerhedskrav og sikkerhedsforanstaltninger

1. Fysiske sikkerhedskrav vælges på grundlag af en trusselvurdering foretaget af Kommissionens sikkerhedsmyndighed, om nødvendigt i samråd med andre kommissionstjenestegrene, andre EU-institutionerne, -agenturer eller -organer og/eller kompetente myndigheder i medlemsstaterne. Kommissionen anvender en risikostyringsproces med henblik på beskyttelse af EUCI på sine lokaliteter for at sikre, at der anvendes en fysisk beskyttelsesgrad, 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 hensyntagen 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 Unionen, dens institutioner, organer eller agenturer eller medlemsstaterne som mål, samt fra sabotage, terrorisme og undergravende eller anden kriminell virksomhed.
2. Kommissionens sikkerhedsmyndighed fastlægger under anvendelse af begrebet dybdeforsvar den rette kombination af de fysiske sikkerhedsforanstaltninger, der skal iværksættes. Kommissionens sikkerhedsmyndighed fastlægger til dette formål minimumsstandarder, normer og kriterier, jf. gennemførelsesbestemmelserne.
3. Kommissionens sikkerhedsmyndighed er bemyndiget til at foretage visitation ved ind- og udgang som afskrækkelse mod uautoriseret indførelse af materiale eller uautoriseret fjernelse af EUCI fra lokaliteter eller bygninger.
4. Hvis der er risiko for indblik i EUCI, selv uforsætligt, skal den pågældende kommissionstjenestegren træffe passende foranstaltninger, som fastlagt af Kommissionens sikkerhedsmyndighed, til at imødegå denne risiko.
5. I forbindelse med nye faciliteter skal fysiske sikkerhedskrav og funktionelle specifikationer fastlægges i samråd med Kommissionens sikkerhedsmyndighed som en del af planlægningen og udformningen af faciliteterne. I forbindelse med eksisterende faciliteter skal fysiske sikkerhedskrav gennemføres i overensstemmelse med minimumsstandarderne, normerne og kriterierne i gennemførelsesbestemmelserne.

Artikel 18

Udstyr til fysisk beskyttelse af EUCI

1. Der etableres to typer fysisk beskyttede områder med henblik på den fysiske beskyttelse af EUCI:
 - a) administrative områder og
 - b) sikrede områder (herunder teknisk sikrede områder).
2. Kommissionens sikkerhedsakkrediteringsmyndighed bestemmer, om et område opfylder kravene til at blive betegnet som et administrativt område, et sikret område eller et teknisk sikret område.
3. Det gælder for administrative områder:
 - a) at der skal etableres en synligt afgrænset perimenter, der muliggør kontrol af personer og om muligt køretøjer
 - b) at uledsaget adgang kun tillades for personer, der er behørigt autoriseret af Kommissionens sikkerhedsmyndighed eller af en anden kompetent myndighed, og
 - c) at alle andre personer til stadighed skal ledsages eller underkastes tilsvarende kontrol.

4. Det gælder for sikrede områder:

- a) at der skal etableres en synligt afgrænset og beskyttet perimenter, hvor al ind- og udgang kontrolleres ved hjælp af et adgangskort eller et persongenkendelsessystem
- b) at uledsaget adgang kun tillades for personer, der er sikkerhedsgodkendt og specifikt autoriseret til at komme ind på området på grundlag af deres need-to-know
- c) at alle andre personer til stadighed skal ledsages eller underkastes tilsvarende kontrol.

5. Hvis adgangen til et sikret område i praksis indebærer direkte adgang til de klassificerede informationer, der opbevares i området, 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 særlig autorisation for 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.

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

- a) sådanne områder skal udstyres med et system til afsløring af indtrængen (»IDS«), være aflåst, når de ikke er i brug, og være bevogtet, når de er i brug. Eventuelle nøgler skal forvaltes i overensstemmelse med artikel 20
- b) alle personer og alt materiel, der kommer ind i disse områder, skal kontrolleres
- c) områderne skal underkastes Kommissionens sikkerhedsmyndigheds regelmæssige fysiske og/eller tekniske inspektioner. Inspektionerne skal desuden foretages efter 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.

7. Inden der 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 stk. 6, litra d), først undersøges af Kommissionens sikkerhedsmyndighed for at sikre, at ingen forståelige informationer uagtsomt eller ulovligt transmitteres ud af det sikrede områdes perimenter ved hjælp af sådant udstyr.

8. 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.

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

10. LSO i den pågældende kommissionstjenestegren udarbejder operationelle sikkerhedsprocedurer (»SecOPs«) for hvert sikret område i overensstemmelse med bestemmelserne i denne afgørelse og gennemførelsesbestemmelserne hertil, hvoraf fremgår:

- a) hvilken EUCI-klassifikationsgrad der kan håndteres og opbevares i området
- b) hvilke overvågnings- og beskyttelsesforanstaltninger der skal opretholdes
- c) hvilke personer der er autoriseret til at få uledsaget adgang til området i kraft af deres need-to-know og sikkerhedsautorisation
- d) hvilke procedurer for ledsagelse eller for sikkerhedsbeskyttelse af EUCI der gælder, når andre personer, hvor dette er relevant, autoriseres til at få adgang til området
- e) hvilke andre foranstaltninger og procedurer der er relevante.

11. Der skal bygges bokslokaler inden for de sikrede områder. Vægge, gulve, lofter, vinduer og låsbare døre skal godkendes af Kommissionens sikkerhedsmyndighed og yde beskyttelse svarende til den, der ydes af en sikkerhedscontainer, der er godkendt til opbevaring af EUCI af samme klassifikationsgrad.

Artikel 19

Fysiske beskyttelsesforanstaltninger med henblik på håndtering og opbevaring af EUCI

1. 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 artikel 31 og har lovet at overholde kompensationsforanstaltningerne i gennemførelsesbestemmelserne, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang.
2. EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, skal opbevares i passende aflåste kontormøbler i et administrativt område eller et sikret område. De kan midlertidigt opbevares uden for et administrativt område eller et sikret område, forudsat at den, der er i besiddelse af informationerne, har lovet at overholde kompensationsforanstaltningerne i gennemførelsesbestemmelserne.
3. 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) har lovet at overholde kompensationsforanstaltningerne i gennemførelsesbestemmelserne, så det sikres, at EUCI er beskyttet mod uautoriserede personers adgang
 - ii) til enhver tid har EUCI under personlig kontrol og
 - iii) i tilfælde af dokumenter i papirform har underrettet det relevante arkiv om situationen.
4. 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.
5. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal opbevares i et sikret område, der etableres og føres af Kommissionens sikkerhedsmyndighed, og som er godkendt til den pågældende grad af Kommissionens sikkerhedsakkrediteringsmyndighed.
6. EUCI, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, skal opbevares i et sikret område, der er godkendt til den pågældende grad af Kommissionens sikkerhedsakkrediteringsmyndighed, på én af følgende måder:
 - a) i en sikkerhedscontainer, jf. artikel 18, med en eller flere af følgende former for supplerende kontrol:
 - 1) permanent beskyttelse eller kontrol foretaget af sikkerhedsgodkendt sikkerhedspersonale eller vagtpersonale
 - 2) et godkendt IDS kombineret med indsatsikkerhedspersonaleeller
 - b) i et bokslokale udstyret med IDS og kombineret med indsatsikkerhedspersonale.

Artikel 20

Forvaltning af nøgler og koder, der anvendes til sikkerhedsbeskyttelse af EUCI

1. Procedurerne for forvaltning af nøgler og koder til kontorer, rum, bokslokaler og sikkerhedscontainere fastlægges i gennemførelsesbestemmelserne i overensstemmelse med artikel 60. Procedurerne skal beskytte mod uautoriseret adgang.
2. Koder skal læres udenad af færrest mulige personer, der har behov for at kende dem. Koder til sikkerhedscontainere og bokslokaler, hvor der opbevares EUCI, skal ændres:
 - a) når der modtages en ny container
 - b) når der sker en ændring i det personale, der kender koden
 - c) når der er konstateret en kompromittering, eller der er mistanke herom
 - d) når der er foretaget vedligeholdelse eller reparation af en lås, og
 - e) mindst hver 12. måned.

KAPITEL 4

FORVALTNING AF EU-KLASSIFICEREDE INFORMATIONER

Artikel 21

Grundprincipper

1. Alle EUCI-dokumenter bør forvaltes i overensstemmelse med Kommissionens politik for dokumentstyring, og de bør derfor registreres, arkiveres, beskyttes og endelig bortskaffes, gemmes i uddrag eller videregives til de historiske arkiver i overensstemmelse med den fælles opbevaringsliste på kommissionsniveau, som gælder for Europa-Kommissionens sager.
2. Informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, sikkerhedsregistreres forud for distributionen og ved modtagelsen. Informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, registreres i dertil oprettede arkiver.
3. Der indføres i Kommissionen et EUCI-arkivsystem i overensstemmelse med artikel 27.
4. De af Kommissionens tjenester og lokaliteter, som håndterer eller opbevarer EUCI, underkastes Kommissionens sikkerhedsmyndigheds regelmæssig inspektion.
5. 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 kapitel 5
 - 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 kapitel 5, eller
 - ii) i alle andre tilfælde som foreskrevet i gennemførelsesbestemmelserne.

Artikel 22

Klassifikation og mærkning

1. Informationer klassificeres, hvis de kræver beskyttelse med hensyn til fortroligheden, jf. artikel 3, stk. 1.
2. Det er udstederen af EUCI, der er ansvarlig for at fastlægge klassifikationsgraden i overensstemmelse med de relevante gennemførelsesbestemmelser, standarder og retningslinjer for klassifikation og for den første udbredelse af informationerne.
3. EUCI-klassifikationsgraden fastlægges i overensstemmelse med artikel 3, stk. 2, og de relevante gennemførelsesbestemmelser.
4. Sikkerhedsklassifikationen skal fremgå klart og korrekt, uanset om EUCI gives i papirform, mundtligt, elektronisk eller i en anden form.
5. De enkelte dele af et dokument (dvs. sider, afsnit, afdelinger, bilag, tillæg og vedhæftet materiale) kan kræve forskellig klassifikationsgrad, og skal mærkes i overensstemmelse hermed, også under opbevaring i elektronisk form.
6. Et dokument 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 berettige til en højere klassifikationsgrad end de enkelte deles klassifikationsgrad.
7. Dokumenter, der indeholder dele med forskellig klassifikationsgrad, skal så vidt muligt struktureres, så dele med en anden klassifikationsgrad let kan identificeres og udskilles, hvis det er nødvendigt.
8. En følgeskrivelse klassificeres lige så højt som bilagenes højeste klassifikationsgrad. Udstederen skal klart 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

*Artikel 23***Mærkning**

Ud over en af de klassifikationsmærkninger, der er nævnt i artikel 3, 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 begrænsninger i anvendelsen
- c) videregivelsespåtegninger
- d) eventuelt den dato eller den specifikke begivenhed, efter hvilken de kan nedklassificeres eller afklassificeres.

*Artikel 24***Forkortede klassifikationsmærkninger**

1. Standardiserede forkortede klassifikationsmærkninger kan anvendes for at angive klassifikationsgraden for de enkelte afsnit af en tekst. Forkortelserne erstatter ikke den uforkortede klassifikationsmærkning.
2. 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

*Artikel 25***Udarbejdelse af EUCI**

1. 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.
2. Hvis stk. 1 ikke kan finde anvendelse på EUCI, træffes der andre passende foranstaltninger i overensstemmelse med gennemførelsesbestemmelserne.

*Artikel 26***Nedklassificering og afklassificering af EUCI**

1. På det tidspunkt, hvor informationerne udarbejdes, angiver udstederen så vidt muligt, om EUCI kan nedklassificeres eller afklassificeres på en bestemt dato eller efter en bestemt begivenhed.
2. Alle kommissionstjenestegrene tager regelmæssigt EUCI, som de har udstedt, op til revision for at vurdere, om klassifikationsgraden fortsat skal finde anvendelse. Der skal ved gennemførelsesbestemmelserne indføres et system, som sikrer, at klassifikationsgraden for registrerede EUCI, som er udstedt af Kommissionen, revideres 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.

3. Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, og som er udstedt af Kommissionen, vil automatisk blive anset for at kunne afklassificeres efter 30 år, jf. forordning (EØF, Euratom) nr. 354/83, ændret ved Rådets forordning (EF, Euratom) nr. 1700/2003 ⁽¹⁾.

Artikel 27

EUCI-arkivsystemet i Kommissionen

1. Med forbehold af artikel 52, stk. 5, skal der i alle kommissionstjenestegrene, som håndterer eller lagrer EUCI i klassifikationsgrad CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, udpeges et ansvarligt lokalt EUCI-arkiv for at sikre, at EUCI håndteres i overensstemmelse med denne afgørelse.

2. Det EUCI-arkiv, der forvaltes af Generalsekretariatet, skal fungere som Kommissionens centrale EUCI-arkiv. Det skal fungere som:

- det lokale EUCI-arkiv for Kommissionens Generalsekretariat
- EUCI-arkiv for kommissionsmedlemmernes kabinetter, medmindre disse har et specifikt lokalt EUCI-arkiv
- EUCI-arkiv for generaldirektorater og tjenester, som ikke har et lokalt EUCI-arkiv
- hovedkanal for ind- og udgående udveksling af alle informationer, der er klassificeret RESTREINT UE/EU RESTRICTED og højere, herunder SECRET UE/EU SECRET, mellem Kommissionen og dens tjenester og tredjelande og internationale organisationer og, når det er fastlagt i særlige ordninger, for andre EU-institutioner, -agenturer og -organer.

3. I Kommissionen udpeger Kommissionens sikkerhedsmyndighed et arkiv, som skal fungere som den centrale modtagelses- og afsendelsesmyndighed for informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET. Der kan i om nødvendigt oprettes underarkiver, der håndterer disse informationer i registreringsøjemed.

4. Underarkiver må ikke sende TRÈS SECRET UE/EU TOP SECRET-dokumenter direkte til andre underarkiver under samme centrale TRÈS SECRET UE/EU TOP SECRET-arkiv eller til anden side uden sidstnævntes udtrykkelige skriftlige godkendelse.

5. EUCI-arkiver skal oprettes som sikrede områder, jf. kapitel 3, og godkendes af Kommissionens sikkerhedsakkrediteringsmyndighed.

Artikel 28

Arkivansvarlig

1. Hvert EUCI-arkiv skal forvaltes af en arkivansvarlig (»RCO«).

2. RCO skal have den relevante sikkerhedsgodkendelse.

3. RCO'en er underlagt et tilsyn, der føres af den lokale sikkerhedsansvarlige i den pågældende tjenestegren i Kommissionen, for så vidt angår anvendelse af bestemmelserne om håndtering af EUCI-dokumenter og efterlevelse af de relevante sikkerhedsregler, standarder og retningslinjer.

4. RCO'en skal som led i forvaltningen af det EUCI-arkiv, vedkommende har ansvaret for, varetage følgende overordnede opgaver i overensstemmelse med denne afgørelse og de relevante gennemførelsesbestemmelser, standarder og retningslinjer:

- forvalte operationer i forbindelse med registrering, bevarelse, reproduktion, oversættelse, transmission, afsendelse og destruktion eller overdragelse til de historiske arkiver af EUCI
- løbende vurdere behovet for at fastholde klassificeringen af informationerne
- varetage andre opgaver med tilknytning til beskyttelsen af EUCI som fastlagt i gennemførelsesbestemmelserne.

Artikel 29

Sikkerhedsregistrering af EUCI

1. I denne afgørelse forstås ved sikkerhedsregistrering (i det følgende benævnt »registrering«) anvendelse af procedurer, som registrerer EUCI's livscyklus, herunder udbredelsen.

⁽¹⁾ Rådets forordning (EF, Euratom) nr. 1700/2003 af 22. september 2003 om ændring af forordning (EØF, Euratom) nr. 354/83 om åbning for offentligheden af de historiske arkiver for Det Europæiske Økonomiske Fællesskab og Det Europæiske Atomenergifællesskab (EUT L 243 af 27.9.2003, s. 1).

2. Alle informationer eller alt materiale, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, skal registreres i dertil oprettede arkiver, når det ankommer til eller forlader en organisatorisk enhed.
3. Når EUCI håndteres eller lagres ved hjælp af et kommunikations- og informationssystem (CIS), kan registreringsprocedurerne foretages af processer i selve CIS.
4. Der fastlægges nærmere bestemmelser om sikkerhedsregistrering af EUCI i gennemførelsesbestemmelserne.

Artikel 30

Kopiering og oversættelse af EUCI-klassificerede dokumenter

1. Dokumenter, der er klassificeret TRÈS SECRET UE/EU TOP SECRET, må kun kopieres eller oversættes med udstederens forudgående skriftlige samtykke.
2. 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.
3. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, gælder også for kopier og oversættelser af det.

Artikel 31

Transport af EUCI

1. EUCI skal transporteres på en måde, der beskytter mod uautoriseret videregivelse under transporten.
2. Transport af EUCI er omfattet af beskyttelsesforanstaltningerne, som skal:
 - svare til klassifikationsgraden af de EUCI, der transporteres, og
 - tilpasses de særlige transportbetingelser, især afhængigt af om EUCI transporteres:
 - i en kommissionsbygning eller inden for en selvstændig gruppe af kommissionsbygninger
 - mellem kommissionsbygninger beliggende i samme medlemsstat
 - inden for Unionen
 - fra Unionen til et tredjelandets område, og
 - tilpasses EUCI's natur og form.
3. Beskyttelsesforanstaltningerne skal fastlægges nærmere i gennemførelsesbestemmelserne, eller hvis der er tale om projekter og programmer omhandlet i artikel 42, som en integrerende del af de relevante program- eller projektsikkerhedsinstruktioner (»PSI«).
4. Gennemførelsesbestemmelserne eller PSI skal omfatte bestemmelser, der svarer til EUCI-klassifikationsgraden med hensyn til:
 - transportformen, f.eks. håndbåret transport eller transport med diplomatisk kurer, militærkurer, posttjenester eller kommercielle kurentjenester
 - pakning af EUCI
 - tekniske modforanstaltninger for EUCI, der transporteres via elektroniske medier
 - eventuelle andre proceduremæssige, fysiske eller elektroniske foranstaltninger
 - registreringsprocedurer
 - brug af sikkerhedsautoriseret personale.
5. Ved transport af EUCI ved hjælp af elektroniske medier kan beskyttelsesforanstaltningerne i de relevante gennemførelsesbestemmelser uanset artikel 21, stk. 5, suppleres med hensigtsmæssige tekniske modforanstaltninger, som er godkendt af Kommissionens sikkerhedsmyndighed med henblik på at minimere risikoen for tab eller kompromittering.

*Artikel 32***Destruktion af EUCI**

1. EU-klassificerede dokumenter, som ikke længere nødvendige, kan destrueres under hensyntagen til forordningerne om arkiver og Kommissionens regler og bestemmelser om dokumentstyring og -arkivering, navnlig den fælles opbevaringsliste på kommissionsniveau.
2. EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL og højere skal destrueres af RCO for det ansvarlige EUCI-arkiv på anmodning af den, der er i besiddelse af dem, eller af en kompetent myndighed. RCO'en ajourfører logbøger og andre registreringsinformationer i overensstemmelse hermed.
3. For så vidt angår dokumenter, der er klassificeret SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, foretager RCO'en destruktionsarbejdet i overværelse af et vidne, der er sikkerhedsgodkendt til mindst samme klassifikationsgrad som det dokumentet, der skal destrueres.
4. Den arkivansvarlige og vidnet, hvis dets tilstedeværelse er påkrævet, underskriver en destruktionsattest, der opbevares i arkivet. RCO'en for det ansvarlige EUCI-arkiv 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 eller SECRET UE/EU SECRET, i en periode på mindst fem år.
5. Klassificerede dokumenter, herunder dem, der er klassificeret RESTREINT UE/EU RESTRICTED, skal destrueres på de måder, der er beskrevet i gennemførelsesbestemmelserne, og som opfylder relevante EU-standarder eller tilsvarende standarder.
6. EDB-lagringsmedier, der anvendes til EUCI, skal destrueres i overensstemmelse med procedurerne i gennemførelsesbestemmelserne.

*Artikel 33***Destruktion af EUCI i nødsituationer**

1. Kommissionstjenestegrene, der er i besiddelse af EUCI, udarbejder på grundlag af lokale forhold planer for sikker opbevaring af EU-klassificeret materiale i krisesituationer, herunder om nødvendigt planer for nøddestruktion eller nødflytning. De skal udbrede de instruktioner, der skønnes nødvendige for at forhindre, at EUCI falder i de forkerte hænder.
2. Foranstaltningerne til sikker opbevaring og/eller destruktion i krisesituationer af EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, må under ingen omstændigheder være til skade for opbevaringen eller destruktionsarbejdet af materiale, der er klassificeret TRÈS SECRET UE/EU TOP SECRET; dette gælder ligeledes krypteringsudstyr, som skal prioriteres højere end alle andre opgaver.
3. Hvis der i en nødsituation er overhængende fare for uautoriseret videregivelse, skal EUCI destrueres af den, der er i besiddelse af informationerne, på en sådan måde, at de ikke kan rekonstrueres hverken helt eller delvis. Udstederen og det udstedende arkiv skal underrettes om destruktionsarbejdet af de registrerede EUCI i den pågældende nødsituation.
4. Der fastlægges nærmere bestemmelser om destruktion af EUCI i gennemførelsesbestemmelserne.

KAPITEL 5

BESKYTTELSE AF EU-KLASSIFICEREDE INFORMATIONER I KOMMUNIKATIONS- OG INFORMATIONSSYSTEMER (CIS)*Artikel 34***Grundprincipper for informationssikring**

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.

2. Effektiv informationssikring sikrer et passende niveau af:

Autenticitet: sikkerhed for, at informationer er ægte og fra bona fide-kilder

Tilgængelighed: det forhold, at informationerne er tilgængelige og kan anvendes på anmodning af en autoriseret enhed

Fortrolighed: det forhold, at informationerne ikke videregives til uautoriserede personer, enheder eller processer

Integritet: sikkerhed for, at informationerne og aktiverne er korrekte og fuldstændige

Uafviselighed: det forhold, at det kan bevises, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes.

3. IA baseres på en risikostyringsproces.

Artikel 35

Definitioner

I dette kapitel forstås ved:

- a) »akkreditering«: den formelle autorisation og godkendelse af et kommunikations- og informationssystem fra sikkerhedsakkrediteringsmyndigheden til at behandle EUCI i dets operationelle miljø efter en formel godkendelse af sikkerhedsplanen og dens korrekte gennemførelse
- b) »akkrediteringsproces«: de skridt og opgaver, der er en forudsætning for sikkerhedsakkrediteringsmyndighedens akkreditering. Disse skridt og opgaver specificeres i en akkrediteringsprocesstandard
- c) »kommunikations- og informationssystem« (CIS): et system, der muliggør håndtering af informationer i elektronisk form. Et kommunikations- og informationssystem omfatter alle aktiver, der er nødvendige for dets drift, herunder infrastruktur, organisation, personale og informationsressourcer
- d) »residualrisiko«: den risiko, der fortsat eksisterer, efter at der er gennemført sikkerhedsforanstaltninger, idet ikke alle trusler imødegås, og ikke alle sårbarheder kan fjernes
- e) »risiko«: muligheden for, at en given trussel vil udnytte indre og ydre sårbarheder i en organisation eller i nogle af de systemer, den 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
- f) »risikoaccept«: beslutningen om at acceptere, at der fortsat findes en residualrisiko efter risikobehandlingen
- g) »risikovurdering«: identifikation af trusler og sårbarheder og udførelse af den dertil knyttede risikoanalyse, dvs. analyse af sandsynlighed og virkning
- h) »risikokommunikation«: udvikling af bevidstheden om risici blandt CIS-brugere, underretning af godkendelsesmyndigheder om sådanne risici og indberetning af dem til driftsmyndigheder
- i) »risikobehandling«: afbødning, fjernelse, reduktion (gennem en passende kombination af tekniske, fysiske, organisatoriske eller proceduremæssige foranstaltninger), flytning eller overvågning af risikoen.

Artikel 36

CIS, der håndterer EUCI

1. CIS håndterer EUCI i overensstemmelse med begrebet IA.

2. Ved CIS, der håndterer EUCI, indebærer efterlevelse af Kommissionens politik for informationssystemssikkerhed, jf. Kommissionens afgørelse C(2006) 3602 ⁽¹⁾:

- a) at tilgangen »planlæg-gennemfør-kontroller-reager« anvendes ved gennemførelse af politikken for informationssystemssikkerhed i informationssystemets fulde livscyklus
- b) at sikkerhedsbehovene identificeres ved hjælp af en aktivitetsmæssig konsekvensanalyse
- c) at informationssystemet og dataene deri skal underkastes en formel klassificering af aktiver

⁽¹⁾ C(2006) 3602 af 16. august 2006 om sikkerheden i de informationssystemer, Europa-Kommissionen anvender.

- d) at alle obligatoriske sikkerhedsforanstaltninger, jf. politikken for informationssystemers sikkerhed, skal gennemføres
 - e) at der anvendes en risikostyringsproces bestående af følgende skridt: identifikation af trusler og sårbarhed, risikovurdering, risikobehandling, risikoaccept og risikokommunikation
 - f) at der udarbejdes en sikkerhedsplan, herunder en sikkerhedspolitik og operationelle sikkerhedsprocedurer, som gennemføres, kontrolleres og revideres.
3. Al personale, der er involveret i udformningen, udviklingen, testningen, driften, forvaltningen eller brugen af CIS, som håndterer EUCI, skal meddele sikkerhedsakkrediteringsmyndigheden alle potentielle sikkerhedssvagheder, hændelser og sikkerhedsbrud eller -kompromittering, som kan have indflydelse på beskyttelsen af CIS og/eller de EUCI, det indeholder.
4. Hvis beskyttelsen af EUCI sker ved hjælp af kryptoprodukter, skal sådanne produkter være godkendt på følgende måde:
- a) der gives fortrinsret til produkter, der er godkendt af Rådet eller af Rådets generaldirektorat i dets virke som Rådets kryptogodkendelsesmyndighed efter henstilling fra Kommissionens sikkerhedsekspertgruppe
 - b) hvis det er berettiget af særlige operative grunde, kan Kommissionens kryptogodkendelsesmyndighed (CAA) efter henstilling fra Kommissionens sikkerhedsekspertgruppe fravige de i litra a) omhandlede krav og give en midlertidig godkendelse for en bestemt periode.
5. Ved elektronisk transmission, behandling og lagring af EUCI skal der anvendes godkendte kryptoprodukter. Uanset dette krav kan der følges specifikke procedurer i nødsituationer eller i specifikke tekniske konfigurationer efter CAA's godkendelse.
6. Der gennemføres sikkerhedsforanstaltninger for at beskytte CIS'er, der håndterer informationer, som er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller højere, mod kompromittering af sådanne informationer gennem utilsigtede elektromagnetiske emissioner («Tempestsikkerhedsforanstaltninger»). Sådanne sikkerhedsforanstaltninger skal svare til risikoen for udnyttelse af informationerne og til informationernes klassifikationsgrad.
7. Kommissionens sikkerhedsmyndighed varetager følgende funktioner:
- IA-myndighed (IAA)
 - Sikkerhedsakkrediteringsmyndighed (SAA)
 - Tempestmyndighed (TA)
 - Kryptogodkendelsesmyndighed (CAA)
 - Kryptodistributionsmyndighed (CDA)
8. Kommissionens sikkerhedsmyndighed udnævner den operative IA-myndighed for hvert system.
9. De opgaver, der hører til funktionerne i stk. 7 og 8, fastlægges i gennemførelsesbestemmelserne.

Artikel 37

Akkreditering af CIS, der håndterer EUCI

1. Alle CIS, der håndterer EUCI, skal underkastes en akkrediteringsproces, som bygger på IA-principperne, og hvis detaljeringsgrad skal svare til den krævede beskyttelsesgrad.
2. Akkrediteringsprocessen skal omfatte den formelle validering, som Kommissionens sikkerhedsakkrediteringsmyndighed foretager af sikkerhedsplanen for det pågældende CIS med henblik på at opnå sikkerhed for:
 - a) at risikostyringsprocessen omhandlet i artikel 36, stk. 2, er korrekt gennemført
 - b) at systemejeren bevidst har accepteret residualrisikoen, og
 - c) at der er opnået et tilstrækkeligt beskyttelsesniveau for CIS og de EUCI, det håndterer, i overensstemmelse med denne afgørelse.

3. Kommissionens sikkerhedsakkrediteringsmyndighed skal udstede en akkrediteringsudredning, som fastsætter den højeste klassifikationsgrad for de EUCI, der kan håndteres i et CIS, og de betingelser og vilkår, der svarer hertil. Dette berører ikke de opgaver, som tilfalder den komité for sikkerhedsgodkendelse, der er omhandlet i artikel 11 i Europa-Parlamentets og Rådets forordning (EU) nr. 512/2014 ⁽¹⁾.
4. Et fælles sikkerhedsakkrediteringsudvalg (SAB) får ansvaret for at akkreditere Kommissionens CIS, der involverer flere parter. Det består af en SAA-repræsentant for hver involveret part og ledes af en SAA-repræsentant for Kommissionen.
5. Akkrediteringsprocessen skal bestå af en række opgaver, der varetages af de involverede parter. Ansvaret for at forberede akkrediteringssager og -dokumentation påhviler udelukkende CIS-systemejer.
6. Ansvaret for akkrediteringen påhviler Kommissionens SAA, som på ethvert tidspunkt i livscyklussen for CIS har ret til:
 - a) at kræve, at der anvendes en akkrediteringsproces
 - b) at foretage en revision eller kontrol af CIS
 - c) såfremt driftsbetingelserne ikke længere er opfyldt, at kræve, at der udarbejdes og effektivt gennemføres en plan for forbedring af sikkerheden inden for en veldefineret frist, eventuelt med tilbagekaldelse af tilladelsen til at drive CIS, indtil driftsbetingelserne igen er opfyldt.
7. Akkrediteringsprocessen skal fastlægges i en standard for akkrediteringsprocessen for CIS, der håndterer EUCI, som skal vedtages i henhold til artikel 10, stk. 3, i afgørelse C(2006) 3602.

Artikel 38

Nødsituationer

1. Uanset bestemmelserne i dette kapitel 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.
2. EUCI kan transmitteres ved hjælp af kryptoprodukter, der er godkendt til en lavere klassifikationsgrad eller endda 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, og
 - b) det klassificerede materiale ikke kan sendes i tide med andre midler.
3. Klassificerede informationer, der transmitteres under de i stk. 1 nævnte omstændigheder, må ikke bære nogen mærkning eller påtegning, der skiller dem ud fra informationer, der er uklassificerede eller kan beskyttes ved hjælp af et disponibelt kryptoprodukt. Modtagerne skal med andre midler straks underrettes om klassifikationsgraden.
4. Der udarbejdes efterfølgende en rapport til den kompetente myndighed og til Kommissionens sikkerhedssektorgruppe.

KAPITEL 6

INDUSTRISIKKERHED

Artikel 39

Grundprincipper

1. Ved industrisikkerhed forstås de foranstaltninger til beskyttelse af EUCI,
 - a) der inden for rammerne af klassificerede kontrakter, anvendes af:
 - i) kandidater eller tilbudsgivere i hele udbuds- og kontraktindgåelsesproceduren
 - ii) kontrahenter eller underkontrahenter i løbet af de klassificerede kontrakters livscyklus

⁽¹⁾ Europa-Parlamentets og Rådets forordning (EU) nr. 512/2014 af 16. april 2014 om ændring af forordning (EU) nr. 912/2010 om oprettelse af Det Europæiske GNSS-agentur (EUT L 150 af 20.5.2014, s. 72).

- b) der inden for rammerne af klassificerede tilskudsftaler, anvendes af:
- i) ansøgere i løbet af proceduren for tildeling af tilskud
 - ii) tilskudsmodtagere i løbet af de klassificerede tilskudsftalers livscyklus.
2. Sådanne kontrakter eller tilskudsftaler må ikke indebære adgang til informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET.
3. Medmindre andet er angivet, finder bestemmelser i dette kapitel, som henviser til klassificerede kontrakter eller kontrahenter, også anvendelse på klassificerede underkontrakter eller underkontrahenter.

Artikel 40

Definitioner

I dette kapitel forstås ved:

- a) »klassificeret kontrakt«: en rammekontrakt eller kontrakt, som omhandlet i Rådets forordning (EF, Euratom) nr. 1605/2002 ⁽¹⁾, der er indgået af Kommissionen eller en af dens tjenestegrene med en kontrahent om levering af løsøre eller fast ejendom, udførelse af arbejder eller levering af tjenester, såfremt dens opfyldelse forudsætter eller indebærer udarbejdelse, håndtering eller lagring af EUCI
- b) »klassificeret underleverandørkontrakt«: en kontrakt, som en af Kommissionens eller dens tjenestegrenes kontrahenter indgår med en anden kontrahent (dvs. underkontrahenten) om levering af løsøre eller fast ejendom, udførelse af arbejder eller levering af tjenesteydelser, såfremt dens opfyldelse forudsætter eller indebærer udarbejdelse, håndtering eller lagring af EUCI
- c) »klassificeret tilskudsftale«: en aftale, hvorved Kommissionen yder et tilskud, jf. første del, afsnit VI, i forordning (EF, Euratom) nr. 1605/2002, såfremt dens opfyldelse forudsætter eller indebærer udarbejdelse, håndtering eller lagring af EUCI
- d) »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 for 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.

Artikel 41

Procedure for klassificerede kontrakter eller tilskudsftaler

1. Hver kommissionstjenestegren sikrer som kontraherende myndighed, at der henvises til minimumsstandarderne for industrisikkerhed i dette kapitel, eller at de indarbejdes i kontrakten, og at de overholdes, når der tildeles klassificerede kontrakter eller tilskudsftaler.
2. Med henblik på stk. 1 søger de kompetente tjenester i Kommissionen rådgivning hos Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed, navnlig dets sikkerhedsdirektorat, og de sikrer, at standardkontrakter, -underleverandørkontrakter og -tilskudsftaler indeholder bestemmelser, som afspejler grundprincipperne og minimumsstandarderne for beskyttelse af EUCI, og som skal overholdes af kontrahenter og underleverandører og af de modtagere af tilskud, der er indgået aftale med.
3. Kommissionen samarbejder tæt med NSA'en, DSA'en eller en anden kompetent myndighed i de pågældende medlemsstater.
4. Når en kontraherende myndighed agter at indlede en procedure med henblik på at indgå en klassificeret kontrakt eller tilskudsftale, skal den søge rådgivning hos Kommissionens sikkerhedsmyndighed om spørgsmål vedrørende procedurens klassificerede karakter og elementer i løbet af alle faser.
5. Skabeloner til og modeller for klassificerede kontrakter og underleverandørkontrakter, klassificerede tilskudsftaler, udbudsbekendtgørelser, vejledning om forhold, der forudsætter facilitetssikkerhedsgodkendelser (»FSC«), program- eller projektsikkerhedsinstruktioner (»PSI«), særlige sikkerhedsbetingelser (»SAL«), besøg, transmission og transport af EUCI, som er omfattet af klassificerede kontrakter eller tilskudsftaler, fastlægges i gennemførelsesbestemmelser om industrisikkerhed efter høring af Kommissionens sikkerhedsekspertgruppe.

⁽¹⁾ Rådets forordning (EF, Euratom) nr. 1605/2002 af 25. juni 2002 om finansforordningen vedrørende De Europæiske Fællesskabers almindelige budget (EFT L 248 af 16.9.2002, s. 1).

6. Kommissionen kan indgå klassificerede kontrakter eller tilskudsaftaler, som overdrager opgaver, der indebærer eller medfører adgang til eller håndtering eller opbevaring af EUCI, til erhvervsdrivende, som er registreret i en medlemsstat eller i et tredjeland, med hvem der er indgået en aftale eller en administrativ ordning i henhold til kapitel 7.

Artikel 42

Sikkerhedselementer i klassificerede kontrakter eller tilskudsaftaler

1. Klassificerede kontrakter eller tilskudsaftaler skal indeholde følgende sikkerhedselementer:

Program- eller projektsikkerhedsinstruktioner

- a) Ved »program- eller projektsikkerhedsinstruktion« (PSI) forstås en liste over sikkerhedsprocedurer, der anvendes i forbindelse med et bestemt program eller projekt for at standardisere sikkerhedsprocedurerne. Den kan revideres i hele programmets/projektets løbetid.
- b) Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed udarbejder en generisk PSI, mens kommissionstjenestegrene med ansvar for programmer eller projekter, som indebærer håndtering eller lagring af EUCI, såfremt det er relevant kan udarbejde særlige PSI'er, som skal bygge på de generiske PSI'er.
- c) Der udarbejdes en særlig PSI specifikt for programmer og projekter, der er kendetegnet ved at have en betydelig spændvidde, størrelse eller kompleksitet eller ved at have mange og/eller forskelligartede kontrahenter eller tilskudsmodtagere og andre partnere og interessenter, f.eks. hvad angår deres retsstilling. Den særlige PSI udarbejdes af den/de kommissionstjenestegren(e) med ansvar for forvaltningen af programmet eller projektet i tæt samarbejde med Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed.
- d) Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed forelægger både den generiske og den særlige PSI for Kommissionens sikkerhedsekspertgruppe med henblik på dens rådgivning.

Særlige sikkerhedsbetingelser

- a) Ved »særlige sikkerhedsbetingelser« (SAL) forstås 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.
- b) De kontraktsspecifikke sikkerhedskrav beskrives i SAL. SAL skal, hvor det er relevant, indeholde klassifikationsvejledningen (»SCG«) og være en integrerende del af en klassificeret kontrakt, underleverandørkontrakt eller tilskudsafale.
- c) SAL skal indeholde bestemmelser om, at kontrahenten og/eller tilskudsmodtageren skal opfylde minimumsstandarderne i denne afgørelse. Den kontraherende myndighed sikrer, at det af SAL fremgår, at manglende overholdelse af disse minimumsstandarder kan udgøre tilstrækkelig grund til, at kontrakten eller tilskudsaftalen opsiges.

2. Både PSI og SAL skal indeholde en SCG som et obligatorisk sikkerhedselement:

- a) Ved »klassifikationsvejledning« forstås et dokument, der beskriver de elementer af et program, et projekt, en kontrakt eller en tilskudsafale, som er klassificerede, med angivelse af de gældende klassifikationsgrader. Klassifikationsvejledningen kan udvides i hele programmets, projektets, kontraktens eller tilskudsaftalens løbetid, og oplysningerne kan om- eller nedklassificeres; når der findes en SCG, skal den indgå i SAL.
- b) Inden der iværksættes et udbud eller tildeles en klassificeret kontrakt, skal kommissionstjenestegrenen som kontraherende myndighed fastsætte klassifikationsgraden for informationer, som skal videregives til kandidater, tilbudsgivere og kontrahenter, samt klassifikationsgraden for informationer, som kontrahenten skal udarbejde. Til dette formål udarbejder den efter konsultation af Kommissionens sikkerhedsmyndighed en SCG, som skal anvendes ved opfyldelsen af kontrakten, jf. denne afgørelse og dens gennemførelsesbestemmelser.

- c) Til fastlæggelse af klassifikationsgraden for de forskellige elementer i en klassificeret kontrakt anvendes følgende principper:
- i) ved udarbejdelsen af en SCG skal kommissionstjenestegrenen 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
 - ii) kontraktens samlede klassifikationsgrad må ikke være lavere end den højeste klassifikationsgrad for dens enkelte elementer og
 - iii) den kontraherende myndighed skal, når det er relevant, samarbejde med medlemsstaternes NSA'er, DSA'er eller andre berørte kompetente sikkerhedsmyndigheder, 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.

Artikel 43

Adgang for kontrahenters og tilskudsmodtagers personale til EUCI

Den kontraherende eller tilskudsgivende myndighed sikrer, at klassificerede kontrakter eller tilskudsaftaler indeholder bestemmelser om, at en kontrahents, underleverandørs eller tilskudsmodtagers personale, der med henblik på opfyldelsen af den klassificerede kontrakt, underleverandørkontrakt eller tilskudsaftale behøver adgang til EUCI, kun indrømmes adgang, hvis:

- a) de er sikkerhedsautoriserede til den relevante grad eller på anden måde er behørigt autoriserede, ved at deres need-to-know er fastslået
- b) de er blevet gjort bekendt med regler og procedurer for sikkerhedsbeskyttelse af EUCI og har anerkendt deres ansvar med hensyn til beskyttelse af sådan informationer
- c) de er sikkerhedsgodkendte til den relevante grad for informationer, der af den respektive NSA, DSA eller en anden kompetent myndighed er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET.

Artikel 44

Facilitetssikkerhedsgodkendelse

1. Ved »facilitetssikkerhedsgodkendelse« (»FSC«) forstås en administrativ afgørelse truffet af en NSA, DSA eller en anden kompetent myndighed om, at en facilitet ud fra et sikkerhedsmæssigt synspunkt kan yde tilstrækkelig beskyttelse af EUCI til en bestemt klassifikationsgrad.

2. Inden en kandidat, tilbudsgiver eller kontrahent eller en tilskudsansøger eller tilskudsmodtager kan få rådighed over eller adgang til EUCI, forelægges der en FSC truffet af NSA'en, DSA'en eller en anden kompetent sikkerhedsmyndighed i en medlemsstat, hvoraf det i overensstemmelse med nationale love og forskrifter fremgår, at en erhvervsdrivende kan beskytte EUCI til den nødvendige klassifikationsgrad (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) på sine faciliteter, for Kommissionens sikkerhedsmyndighed, som denne videresender til den kommissionstjenestegren, der fungerer som kontraherende eller tilskudsgivende myndighed.

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

4. Den kontraherende eller tilskudsgivende myndighed tildeler ikke en klassificeret kontrakt eller en tilskudsaftale til en udvalgt tilbudsgiver eller deltager, før den fra NSA'en, DSA'en eller anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor den pågældende kontrahent eller underleverandør er registreret, har fået bekræftet, at der er udstedt en relevant FSC, hvor dette er påkrævet.

5. Når Kommissionens sikkerhedsmyndighed af en NSA, DSA eller en anden kompetent sikkerhedsmyndighed, som har meddelt en FSC, er blevet underrettet om ændringer, der vil påvirke FSC'en, skal den underrette den kommissionstjenestegren, der fungerer som kontraherende eller tilskudsgivende myndighed. I tilfælde af en underleverandørkontrakt underrettes NSA'en, DSA'en eller en anden kompetent sikkerhedsmyndighed tilsvarende.

6. Hvis den relevante NSA, DSA eller en anden kompetent sikkerhedsmyndighed inddrager en FSC, er det tilstrækkelig grund til, at den kontraherende eller den tilskudsgivende myndighed ophæver en klassificeret kontrakt eller udelukker en kandidat, tilbudsgiver eller ansøger fra udvælgelsen. Der indsættes en bestemmelse herom i de standardkontrakter og -tilskudscontrakter, der udarbejdes.

Artikel 45

Bestemmelser for klassificerede kontrakter eller tilskudscontrakter

1. Hvis EUCI videregives til en kandidat, en tilbudsgiver eller en ansøger i løbet af udbudsproceduren, skal indkaldelsen af udbud eller forslagsindkaldelsen indeholde en bestemmelse om, at kandidater, tilbudsgivere eller ansøgere, som undlader at afgive bud eller forslag, eller som ikke udvælges, har pligt til returnere alle klassificerede dokumenter inden for en bestemt tidsfrist.

2. Den kontraherende eller tilbudsgivende myndighed skal gennem Kommissionens sikkerhedsmyndighed meddele den kompetente NSA, DSA eller en anden kompetent myndighed, at der er tildelt en klassificeret kontrakt eller indgået en tilskudscontrakte, samt de relevante oplysninger, såsom kontrahentens eller støttemodtagerens navn, kontraktens varighed og højeste klassifikationsgrad.

3. Når sådanne kontrakter eller tilskudscontrakter afsluttes, skal den kontraherende eller tilbudsgivende myndighed straks via Kommissionens sikkerhedsmyndighed underrette NSA'en, DSA'en eller en anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor kontrahenten eller tilskudsmodtageren er registreret.

4. Som hovedregel er kontrahenten eller tilskudsmodtageren forpligtet til at returnere EUCI, som vedkommende er i besiddelse af, til den kontraherende eller tilskudsgivende myndighed ved ophævelsen af den klassificerede kontrakt eller tilskudscontrakte.

5. De særlige bestemmelser for bortskaffelse af EUCI under opfyldelsen af den klassificerede kontrakt eller aftale eller ved dens ophævelse fastsættes i SAL.

6. Er kontrahenten eller tilskudsmodtageren autoriseret til at beholde EUCI efter den klassificerede kontrakt eller tilskudscontraktens ophævelse, skal minimumsstandarderne i denne afgørelse fortsat opfyldes, og kontrahenten eller tilskudsmodtageren skal beskytte EUCI's fortrolighed.

Artikel 46

Særlige bestemmelser for klassificerede kontrakter

1. De betingelser, der er relevante for beskyttelsen af EUCI, og hvorpå kontrahenten kan udbyde dele af kontrakten til underleverandører, skal fastsættes i udbuddet og i den klassificerede kontrakt.

2. En kontrahent skal indhente tilladelse fra den kontraherende myndighed, inden en del af en klassificeret kontrakt udbydes til underleverandører. Ingen underleverandørkontrakt, som indebærer adgang til EUCI, må tildeles til underleverandører, der er registrerede i et tredjeland, medmindre der findes et regelsæt for beskyttelsen af informationerne, jf. kapitel 7.

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

4. For så vidt angår EUCI, der udarbejdes eller håndteres af kontrahenten, skal Kommissionen anses for at være udsteder, og de rettigheder udsteder har, skal udøves af den kontraherende myndighed.

Artikel 47

Besøg i forbindelse med klassificerede kontrakter

1. Hvis Kommissionens, kontrahenters eller tilskudsmodtagerens personale skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, i hinandens lokalteter med henblik på opfyldelse af en klassificeret kontrakt eller tilskudscontrakte, skal besøg tilrettelægges i samråd med de pågældende NSA'er, DSA'er eller andre berørte kompetente sikkerhedsmyndigheder. Kommissionens sikkerhedsmyndighed skal underrettes om sådanne besøg. I forbindelse med specifikke programmer eller projekter kan NSA'er, DSA'er eller andre kompetente sikkerhedsmyndigheder dog også aftale en procedure, hvorved sådanne besøg kan tilrettelægges direkte.

2. Alle besøgende skal være i besiddelse af en relevant PSC og have need-to-know med henblik på adgang til EUCI vedrørende den klassificerede kontrakt.
3. Besøgende gives kun adgang til EUCI, der har relation til besøgets formål.
4. De nærmere bestemmelser fastlægges i gennemførelsesbestemmelserne.
5. Det er obligatorisk at overholde bestemmelserne vedrørende besøg i forbindelse med klassificerede kontrakter i denne afgørelse og de i stk. 4 omhandlede gennemførelsesbestemmelser.

Artikel 48

Transmission og transport af EUCI i forbindelse med klassificerede kontrakter eller klassificerede tilskudsaftaler

1. For så vidt angår elektronisk transmission af EUCI anvendes de relevante bestemmelser i afgørelsens kapitel 5.
2. For så vidt angår transport af EUCI, finder de relevante bestemmelser i afgørelsens kapitel 4 og dens gennemførelsesbestemmelser anvendelse i overensstemmelse med nationale love og bestemmelser.
3. For så vidt angår fragtttransport af klassificeret materiale anvendes følgende principper ved fastlæggelsen af sikkerhedsforanstaltninger:
 - a) sikkerheden skal garanteres på alle stadier under transporten fra udgangspunktet til det endelige bestemmelsessted
 - b) den grad af beskyttelse, en forsendelse ydes, bestemmes af den højeste klassifikationsgrad for det materiale, den indeholder
 - c) 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 en anden berørt kompetent sikkerhedsmyndighed
 - d) transporten gennemføres så vidt muligt direkte og afsluttes så hurtigt, som forholdene tillader
 - e) 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 en anden kompetent sikkerhedsmyndighed i såvel afsenderens som modtagerens stat har givet tilladelse hertil.

Artikel 49

Videregivelse af EUCI til kontrahenter eller tilskudsmodtagere i tredjelande

EUCI videregives til kontrahenter eller tilskudsmodtagere i tredjelande i overensstemmelse med de sikkerhedsforanstaltninger, der er aftalt mellem Kommissionens sikkerhedsmyndighed og kommissionstjenestegrenen som kontraherende myndighed eller tilskudsmyndighed og NSA'en, DSA'en eller en anden kompetent sikkerhedsmyndighed i det pågældende tredjeland, hvor kontrahenten eller tilskudsmodtageren er registreret.

Artikel 50

Håndtering af information, der er klassificeret RESTREINT UE/EU RESTRICTED, i forbindelse med klassificerede kontrakter eller klassificerede tilskudsaftaler

1. Beskyttelse af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, og som håndteres eller lagres i forbindelse med klassificerede kontrakter eller tilskudsaftaler, skal bygge på principper om proportionalitet og omkostningseffektivitet.
2. Der kræves ikke FSC eller PSC i forbindelse med klassificerede kontrakter eller klassificerede tilskudsaftaler, som indebærer håndtering af informationer med klassifikationsgraden RESTREINT UE/EU RESTRICTED.
3. Hvis en kontrakt eller en tilskudsaftale indebærer håndtering af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, i et CIS, som drives af en kontrahent eller en tilskudsmodtager, skal den kontraherende eller tilskudsydende myndighed efter høring af Kommissionens sikkerhedsmyndighed sikre, at kontrakten eller tilskudsaftalen i detaljer beskriver de tekniske og administrative krav, der er nødvendige for akkreditering af CIS'et svarende til den vurderede risiko, under hensyntagen til alle relevante faktorer. Omfanget af akkrediteringen eller godkendelsen af et CIS aftales mellem Kommissionens sikkerhedsmyndighed og den relevante NSA eller DSA.

KAPITEL 7

UDVEKSLING AF KLASSIFICEREDE INFORMATIONER MED ANDRE EU-INSTITUTIONER, -AGENTURER, -ORGANER OG -KONTORER, MED MEDLEMSSTATER OG MED TREDJELANDE OG INTERNATIONALE ORGANISATIONER*Artikel 51***Grundprincipper**

1. Hvis Kommissionen eller en af dens tjenestegrene beslutter, at der er behov for at udveksle EUCI med andre EU-institutioner, -agenturer, -organer eller -kontorer eller med et tredjeland eller en international organisation, træffes de nødvendige foranstaltninger til at fastlægge hensigtsmæssige retlige eller administrative regler til formålet, som kan omfatte aftaler eller administrative ordninger om informationssikkerhed, der er indgået i overensstemmelse med de relevante bestemmelser.
2. Med forbehold af artikel 57 må EUCI kun udveksles med andre EU-institutioner, -agenturer, -organer eller -kontorer eller med et tredjeland eller en international organisation, forudsat at der er fastlagt sådanne hensigtsmæssige retlige eller administrative regler, og at der er tilstrækkelig garanti for, at de pågældende EU-institutioner, -agenturer, -organer eller -kontorer eller det pågældende tredjeland eller den pågældende internationale organisation anvender tilsvarende grundprincipper og minimumsstandarder for beskyttelse af klassificerede oplysninger.

*Artikel 52***Udveksling af EUCI med andre EU-institutioner, -agenturer, -organer og -kontorer**

1. Inden Kommissionen fastlægger en administrativ ordning for udveksling af EUCI med andre EU-institutioner, -agenturer, -organer eller -kontorer, skal den sikre sig, at den pågældende EU-institution eller det pågældende EU-agentur, -organ eller -kontor:
 - a) har etableret et regelsæt for beskyttelse af EUCI, som fastlægger grundprincipper og minimumsstandarder svarende til dem, der er fastlagt i denne afgørelse og dens gennemførelsesbestemmelser
 - b) anvender sikkerhedsstandarder og retningslinjer vedrørende personelsikkerhed, fysisk sikkerhed, forvaltning af EUCI og beskyttelse af kommunikations- og informationssystemer (CIS), som garanterer et beskyttelsesniveau svarende til niveauet i Kommissionen
 - c) mærker klassificerede informationer, som den/det udarbejder, som EUCI.
2. Generaldirektoratet for Menneskelige Ressourcer og Sikkerhed er i tæt samarbejde med de øvrige kompetente kommissionstjenestegrene den ledende tjeneste i Kommissionen i forbindelse med indgåelsen af administrative ordninger for udveksling af EUCI med andre EU-institutioner, -agenturer, -organer eller -kontorer.
3. De administrative ordninger skal generelt tage form af en udveksling af breve undertegnet af generaldirektøren for menneskelige ressourcer og sikkerhed på Kommissionens vegne.
4. Inden der indgås en administrativ ordning om udveksling af EUCI, foretager Kommissionens sikkerhedsmyndighed et vurderingsbesøg for at vurdere regelsættet for beskyttelse af EUCI og for at vurdere, om de foranstaltninger, der er truffet for at beskytte EUCI, er effektive. Den administrative ordning må kun træde i kraft, og EUCI må kun udveksles, hvis resultatet af vurderingsbesøget er tilfredsstillende, og hvis de henstillinger, der er givet i forlængelse af besøget, er efterlevet. Der foretages regelmæssige opfølgende vurderingsbesøg for at kontrollere, at den administrative ordning følges, og at sikkerhedsforanstaltningerne fortsat opfylder de aftalte grundprincipper og minimumsstandarder.
5. I Kommissionen skal EUCI-arkivet, som forvaltes af generalsekretariatet, generelt være hovedkanal for ind- og udgående udveksling af klassificerede oplysninger med andre EU-institutioner, -agenturer, -organer eller -kontorer. Hvis det imidlertid af sikkerhedsmæssige, organisatoriske eller driftsmæssige årsager er mere hensigtsmæssigt for beskyttelsen af EUCI, skal de lokale EUCI-arkiver, der er oprettet i kommissionstjenestegrene i overensstemmelse med denne afgørelse og dens gennemførelsesbestemmelser, fungere som kanal for ind- og udgående klassificerede oplysninger vedrørende de anliggender, der hører under de pågældende kommissionstjenestegrenes kompetence.
6. Kommissionens sikkerhedsekspertgruppe underrettes om processen for indgåelse af administrative ordninger, jf. stk. 2.

*Artikel 53***Udveksling af EUCI med medlemsstater**

1. EUCI må udveksles med og videregives til medlemsstater, forudsat at disse beskytter oplysningerne i overensstemmelse med de krav, der gælder for klassificerede informationer med en national klassifikationsmærkning af tilsvarende grad, jf. den sammenlignende oversigt over sikkerhedsklassifikationer i bilag I.
2. Hvis medlemsstaterne bringer klassificerede informationer med en national klassifikationsmærkning ind i Den Europæiske Unions struktur eller netværk, beskytter Kommissionen disse informationer i overensstemmelse med de krav, der gælder for EUCI af en tilsvarende grad, jf. den sammenlignende oversigt over sikkerhedsklassifikationer i bilag I.

*Artikel 54***Udveksling af EUCI med tredjelande og internationale organisationer**

1. Hvis Kommissionen beslutter, at der er et vedvarende behov for at udveksle klassificerede informationer med tredjelande eller internationale organisationer, træffes de nødvendige foranstaltninger til at fastlægge hensigtsmæssige retlige eller administrative regler til formålet, som kan omfatte aftaler eller administrative ordninger om informations-sikkerhed, der er indgået i overensstemmelse med de relevante bestemmelser.
2. Sådanne aftaler og administrative ordninger om informationssikkerhed, jf. stk. 1, skal indeholde bestemmelser, der sikrer, at tredjelande eller internationale organisationer, når de modtager EUCI, sikkerhedsbeskytter sådanne informationer i overensstemmelse med informationernes klassifikationsgrad og efter minimumsstandards, som svarer til de standarder, der er fastlagt i denne afgørelse.
3. Kommissionen kan indgå administrative ordninger i overensstemmelse med artikel 56, hvis klassifikationsgraden for de EUCI, der skal videregives, generelt ikke er højere end RESTREINT UE/EU RESTRICTED.
4. Administrative ordninger for udveksling af klassificerede informationer, jf. stk. 3, skal indeholde bestemmelser, der sikrer, at tredjelande eller internationale organisationer, når de modtager EUCI, sikkerhedsbeskytter sådanne informationer i overensstemmelse med informationernes klassifikationsgrad og efter minimumsstandards svarende til de standarder, der er fastlagt i denne afgørelse. Kommissionens sikkerhedsekspertgruppe skal høres om indgåelsen af aftaler eller administrative ordninger om beskyttelse af informationer.
5. Afgørelsen om at videregive EUCI, der er udstedt i Kommissionen, til et tredjeland eller en international organisation, træffes af kommissionstjenestegrenen fra sag til sag på grundlag af informationernes art og indhold, modtagerens need-to-know og Unionens interesse i videregivelsen. Hvis udstederen af de klassificerede informationer, der ønskes videregivet, eller det kildemateriale, disse kan indeholde, ikke er Kommissionen, skal kommissionstjenestegrenen først indhente udstederens skriftlige samtykke til videregivelsen. Hvis det ikke kan fastslås, hvem der er udsteder, påtager kommissionstjenestegrenen sig udsteders ansvar efter høring af Kommissionens sikkerhedsekspertgruppe.

*Artikel 55***Informationssikkerhedsaftaler**

1. Informationssikkerhedsaftaler med tredjelande eller internationale organisationer indgås i overensstemmelse med TEUF's artikel 218.
2. Informationssikkerhedsaftaler skal:
 - a) fastlægge grundprincipperne og minimumsstandards for udveksling af klassificerede informationer mellem Unionen og et tredjeland eller en international organisation
 - b) indeholde bestemmelser om tekniske gennemførelsesordninger, der aftales mellem de kompetente sikkerhedsmyndigheder i de relevante EU-institutioner og -organer 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
 - c) fastsætte, at det inden udvekslingen af klassificerede informationer i henhold til aftalen skal være konstateret, at den modtagende part vil kunne beskytte og sikre de klassificerede informationer, der videregives, på passende måde.

3. Kommissionen hører, når det i henhold til artikel 51, stk. 1, besluttet, at der er et behov for at udveksle klassificerede informationer, Tjenesten for EU's Optræden Udadtil, Rådets generalsekretariat og andre EU-institutioner og -organer, hvis det er hensigtsmæssigt, for at fastslå, om en henstilling i henhold til artikel 218, stk. 3, i TEUF bør forelægges.
4. EUCI må ikke udveksles elektronisk, medmindre det udtrykkeligt er fastsat i informationssikkerhedsaftalen eller de tekniske gennemførelsesordninger.
5. I Kommissionen skal EUCI-arkivet, som forvaltes af generalsekretariatet, generelt være hovedkanal for ind- og udgående udveksling af klassificerede oplysninger med tredjelande og internationale organisationer. Hvis det imidlertid af sikkerhedsmæssige, organisatoriske eller driftsmæssige årsager er mere hensigtsmæssigt for beskyttelsen af EUCI, skal de lokale EUCI-arkiver, der er oprettet i kommissionstjenestegrenene i overensstemmelse med denne afgørelse og dens gennemførelsesbestemmelser, fungere som kanal for ind- og udgående klassificerede oplysninger vedrørende de anliggender, der hører under de pågældende kommissionstjenestegrenes kompetence.
6. For at vurdere, om sikkerhedsforskrifterne, -strukturerne og -procedurerne i det pågældende tredjeland eller den pågældende internationale organisation er effektive, deltager Kommissionen sammen med andre EU-institutioner, -agenturer eller -organer i vurderingsbesøg efter fælles aftale med tredjelandet eller den internationale organisation. På sådanne vurderingsbesøg skal følgende evalueres:
 - a) regelsættet for sikkerhedsbeskyttelsen af klassificerede informationer
 - b) de særlige kendetegn ved sikkerhedspolitikken og den måde, hvorpå sikkerheden er organiseret i tredjelandet eller den internationale organisation, som kan have indflydelse på klassifikationsgraden for de informationer, der kan udveksles
 - c) de sikkerhedsforanstaltninger og -procedurer, der reelt er indført, og
 - d) sikkerhedsgodkendelsesprocedurerne i forbindelse med klassifikationsgraden for de EUCI, der skal videregives.

Artikel 56

Administrative ordninger

1. Hvis der i forbindelse med EU-politikker eller EU-regler er et vedvarende behov for udveksling af klassificerede informationer, der som hovedregel ikke klassificeres højere end RESTREINT UE/EU RESTRICTED, med et tredjeland eller en international organisation, og Kommissionens sikkerhedsmyndighed efter høring af Kommissionens sikkerhedsekspertgruppe har fastslået, at den pågældende parts sikkerhedssystem ikke er tilstrækkelig udviklet til, at der kan indgås en informationssikkerhedsaftale, kan Kommissionen beslutte at indgå en administrativ ordning med de relevante myndigheder i det pågældende tredjeland eller den pågældende internationale organisation.
2. Administrative ordninger skal som hovedregel have form af en brevveksling.
3. Der skal aflægges et vurderingsbesøg, inden ordningen indgås. Kommissionens sikkerhedsekspertgruppe skal underrettes om resultatet af vurderingsbesøget. Hvis der foreligger ekstraordinære grunde til hurtig udveksling af klassificerede informationer, kan EUCI videregives, på betingelse af at alle bestræbelser sættes ind på at foretage et sådant vurderingsbesøg hurtigst muligt.
4. EUCI må ikke udveksles elektronisk, medmindre det udtrykkeligt er fastsat i den administrative ordning.

Artikel 57

Ekstraordinær ad hoc-videregivelse af EUCI

1. Hvis der ikke foreligger en aftale eller en administrativ ordning om informationssikkerhed, og hvis Kommissionen eller en af dens tjenestegrene fastslår, at der i forbindelse med EU-politikker eller EU-regler er et særligt behov for at videregive EUCI til et tredjeland eller en international organisation, skal Kommissionens sikkerhedsmyndighed så vidt muligt sammen med sikkerhedsmyndighederne i det pågældende tredjeland eller den pågældende internationale organisation kontrollere, at tredjelandets eller organisationens sikkerhedsregler, -strukturer og -procedurer er af en sådan karakter, at EUCI, som videregives til det/den, vil blive beskyttet efter standarder, der er lige så høje som standarderne i denne afgørelse.
2. Kommissionen træffer afgørelse om at videregive EUCI til det pågældende tredjeland eller den pågældende internationale organisation efter høring af Kommissionens sikkerhedsekspertgruppe på grundlag af et forslag fra det medlem af Kommissionen, der er ansvarligt for sikkerhedsanliggender.

3. Når Kommissionens har truffet afgørelse om at videregive EUCI, og forudsat at der foreligger skriftligt samtykke fra udstederen, herunder fra udstederne af eventuelt kildemateriale, som EUCI måtte indeholde, videresender den kompetente kommissionstjenestegren de pågældende informationer, som skal være forsynet med en videregivelses-påtegning, der angiver det tredjeland eller den internationale organisation, som informationerne videregives til. Inden eller ved den faktiske videregivelse skal den berørte tredjepart skriftligt give tilsagn om at beskytte de EUCI, den modtager, i overensstemmelse med grundprincipperne og minimumsstandarderne i denne afgørelse.

KAPITEL 8

AFSLUTTENDE BESTEMMELSER

Artikel 58

Ophævelse af tidligere afgørelse

Denne afgørelse ophæver og træder i stedet for Kommissionens afgørelse 2001/844/EF, EKSF, Euratom ⁽¹⁾.

Artikel 59

Klassificerede informationer, der er udarbejdet inden denne afgørelses ikrafttræden

1. Alle EUCI, der er klassificeret i overensstemmelse med afgørelse 2001/844/EF, EKSF, Euratom, sikkerhedsbeskyttes fortsat i overensstemmelse med de relevante bestemmelser i nærværende afgørelse.
2. Alle klassificerede informationer, som Kommissionen var i besiddelse af på den dato, hvor afgørelse 2001/844/EF, EKSF, Euratom trådte i kraft, skal med undtagelse af Euratom-klassificerede informationer:
 - a) hvis de er udarbejdet af Kommissionen, fortsat pr. definition anses for at være omklassificeret RESTREINT UE, medmindre forfatteren inden den 31. januar 2002 besluttede at give en anden klassifikation og underrettede alle modtagere af det pågældende dokument
 - b) hvis de er udarbejdet af personer uden for Kommissionen, beholde deres oprindelige klassifikationsgrad og således behandles som EUCI af tilsvarende klassifikationsgrad, medmindre forfatteren giver samtykke til afklassificering eller nedklassificering af oplysningerne.

Artikel 60

Gennemførelsesbestemmelser og sikkerhedsmeddelelser

1. Vedtagelsen af gennemførelsesbestemmelserne til denne afgørelse vil efter behov være genstand for en særskilt kommissionsafgørelse om bemyndigelse til fordel for det medlem af Kommissionen, der er ansvarligt for sikkerhedsanliggender, i fuld overensstemmelse med forretningsordenen.
2. Når det pågældende kommissionsmedlem med ansvar for sikkerhedsanliggender har fået bemyndigelse i henhold til ovenfor nævnte kommissionsafgørelse, kan vedkommende udarbejde sikkerhedsmeddelelser, som fastlægger sikkerhedsretningslinjer og bedste praksis inden for denne afgørelses og dens gennemførelsesbestemmelser anvendelsesområde.
3. Kommissionen kan uddelegere opgaverne i stk. 1 og 2 til generaldirektøren for menneskelige ressourcer og sikkerhed ved en særskilt afgørelse om uddelegering i fuld overensstemmelse med forretningsordenen.

Artikel 61

Ikrafttræden

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

Udfærdiget i Bruxelles, den 13. marts 2015.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

⁽¹⁾ Kommissionens afgørelse 2001/844/EF, EKSF, Euratom af 29. november 2001 om ændring af dens forretningsorden (EFT L 317 af 3.12.2001, s. 1).

BILAG I

SAMMENLIGNING AF SIKKERHEDSKLASSIFIKATIONER

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA 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)	Se fodnote (1)
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Tjekkiet	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	Streng geheim	Geheim	VS (?) — Vertraulich	VS — Nur für den Dienstgebrauch
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irland	Top Secret	Secret	Confidential	Restricted
Grækenland	Ακρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Frankrig	Très Secret Défense	Secret Défense	Confidentiel Défense	Se fodnote (2)
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Cypern	Ακρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (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-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederlandene	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Østrig	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Rumænien	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenien	Strogo tajno	Tajno	Zaupno	Interno
Slovakiet	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLI	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sverige (*)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Det Forenede Kongerige	UK TOP SECRET	UK SECRET	Ingen ækvivalens (5)	UK OFFICIAL — SENSITIVE

(1) Diffusion Restreinte/Beperkte Verspreiding er ikke en klassifikation i Belgien. Belgien håndterer og beskytter informationer klassificeret »RESTREINT UE/EU RESTRICTED« efter standarder og procedurer, der er lige så høje, som dem der beskrevet i Rådet for Den Europæiske Unions sikkerhedsregler.

(2) Tyskland: VS = Verschlusssache.

(3) Frankrig anvender ikke klassifikationen »RESTREINT« i sit nationale system. Frankrig håndterer og beskytter informationer klassificeret »RESTREINT UE/EU RESTRICTED« efter standarder og procedurer, der er lige så høje som dem, der beskrevet i Rådet for Den Europæiske Unions sikkerhedsregler.

(4) Sverige: klassifikationsmærkningerne i øverste linje anvendes af forsvarsmyndighederne, mens klassifikationsmærkningerne i nederste linje anvendes af de øvrige myndigheder.

(5) Det Forenede Kongerige håndterer og beskytter EUCI klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL i overensstemmelse med beskyttelseskravene for UK SECRET.

BILAG II

LISTE OVER FORKORTELSER

Forkortelse	Betydning
CA	Kryptomyndighed
CAA	Kryptogodkendelsesmyndighed
CCTV	Intern TV-overvågning
CDA	Kryptodistributionsmyndighed
CIS	Kommunikations- og informationssystemer til håndtering af EUCI
DSA	Udpeget sikkerhedsmyndighed
EUCI	EU's klassificerede informationer
FSC	Facilitetssikkerhedsgodkendelse
IA	Informationssikring
IAA	Informationssikringsmyndighed
IDS	System til afsløring af indtrængen
IT	Informationsteknologi
LSO	Lokal sikkerhedsansvarlig
NSA	National sikkerhedsmyndighed
PSC	Personelsikkerhedsgodkendelse
PSCC	Certifikat for personelsikkerhedsgodkendelse
PSI	Program-/projektsikkerhedsinstruktioner
RCO	Arkivansvarlig
SAA	Sikkerhedsakkrediteringsmyndighed
SAL	Særlige sikkerhedsbetingelser
SCG	Klassifikationsvejledning
SecOPs	Operationelle sikkerhedsprocedurer
TA	Tempestmyndighed
TFEU	Traktaten om Den Europæiske Unions funktionsmåde

BILAG III

LISTE OVER NATIONALE SIKKERHEDSMYNDIGHEDER

BELGIEN

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et
Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tlf. Secrétariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIEN

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tlf. +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Websted: www.dksi.bg

TJEKKIET

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tlf. +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

DANMARK

Politiets Efterretningstjeneste
Klausdalsbrovej 1
2860 Søborg
Tlf. +45 33148888
Fax +45 33430190
Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø
Tlf. +45 33325566
Fax +45 33931320

TYSKLAND

Bundesministerium des Innern
Referat OS III 3
Alt-Moabit 101 D
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 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GRÆKENLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΤ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 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

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

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

4 Emanuel Roidi street

1432 Nicosia

Tlf. +357 22807569, +357 22807643,

+357 22807764

Fax +357 22302351

E-mail: cynsa@mod.gov.cy

KROATIEN

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagreb

Croatia

Tlf. +385 14681222

Fax + 385 14686049

Websted: www.uvns.hr

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

IRLAND

National Security Authority

Department of Foreign Affairs

76 — 78 Harcourt Street

Dublin 2

Tlf. +353 14780822

Fax +353 14082959

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. +370 706 66701, +370 706 66702

Fax +370 706 66700

E-mail: nsa@vsd.lt

ITALIEN

Presidenza del Consiglio dei Ministri

D.I.S. — U.C.Se.

Via di Santa Susanna, 15

00187 Roma

Tlf. +39 0661174266

Fax +39 064885273

LUXEMBOURG

Autorité nationale de Sécurité

Boîte postale 2379

1023 Luxembourg

Tlf. +352 24782210 central

+ 352 24782253 direct

Fax +352 24782243

CYPERN

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Τηλέφωνο: +357 22807569, +357 22807643,

+357 22807764

Τηλεομοιότυπο: +357 22302351

UNGARN

Nemzeti Biztonsági Felügyelet

(National Security Authority of Hungary)

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tlf. +36 (1) 7952303

Fax +36 (1) 7950344

Postadresse:

H-1357 Budapest, PO Box 2

E-mail: nbf@nbf.hu

Websted: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tlf. +356 21249844
Fax +356 25695321

1 300-342 Lisboa
Tlf. +351 213031710
Fax +351 213031711

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

RUMÆNIEN

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tlf. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Websted: www.orniss.ro

ØSTRIG

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tlf. +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

SLOVENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tlf. +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

POLEN

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tlf. +48 22 58 57 944
fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Websted: www.abw.gov.pl

SLOVAKIET

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tlf. +421 268692314
Fax +421 263824005
Websted: www.nbusr.sk

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tlf. 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SVERIGE

Utrikesdepartementet

(Ministry for Foreign Affairs)

SSSB

SE-103 39 Stockholm

Tlf. +46 84051000

Fax +46 87231176

E-mail: ud-nsa@foreign.ministry.se

DET FORENEDE KONGERIGE

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
