1.4.2014 DA Den Europæiske Unions Tidende C 96/1

II

(Meddelelser)

MEDDELELSER FRA DEN EUROPÆISKE UNIONS INSTITUTIONER, ORGANER, KONTORER OG AGENTURER

EUROPA-PARLAMENTET

EUROPA-PARLAMENTETS PRÆSIDIUMS AFGØRELSE

af 15. april 2013

vedrørende regler om Europa-Parlamentets behandling af fortrolige oplysninger

(2014/C 96/01)

EUROPA-PARLAMENTETS PRÆSIDIUM HAR

under henvisning til Europa-Parlamentets forretningsordens artikel 23, stk. 12,

ud fra følgende betragtninger:

(1) I lyset af den nye rammeaftale om forbindelserne mellem Europa-Parlamentet og Europa-Kommissionen ([1]), som blev undertegnet den 20. oktober 2010 (»Rammeaftalen«) og af den interinstitutionelle aftale mellem Europa-Parlamentet og Rådet om fremsendelse til Europa-Parlamentet og dettes behandling af Rådets klassificerede informationer på andre områder end dem, der er omfattet af den fælles udenrigs- og sikkerhedspolitik ([2]) undertegnet den 12. marts 2014 (»den interinstitutionelle aftale«) er det blevet nødvendigt at opstille særlige regler om Europa-Parlamentets behandling af fortrolige oplysninger.

(2) Lissabontraktaten tillægger Europa-Parlamentet nye opgaver, og det er med henblik på at udvikle Parlamentets aktiviteter på områder, der kræver fortrolighed, nødvendigt at fastlægge grundlæggende principper, minimumstandarder for sikkerhed og passende procedurer for Europa-Parlamentets behandling af fortrolige, herunder klassificerede, oplysninger.

(3) Formålet med reglerne i denne afgørelse er at sikre ensartede beskyttelsesstandarder og forenelighed med de regler, der er vedtaget af andre institutioner, organer, kontorer og agenturer, der er oprettet med hjemmel i traktaterne, eller af medlemsstaterne, for at gøre det lettere for EU's beslutningsproces at fungere tilfredsstillende.

(4) Reglerne i denne afgørelse berører ikke nuværende og fremtidige regler om aktindsigt, vedtaget i overensstemmelse med artikel 15 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

([1]) EUT L 304 af 20.11.2010, s. 47.
([2]) EUT C 95 af 1.4.2014, s. 1.

(5) Reglerne i denne afgørelse berører ikke nuværende og fremtidige regler om beskyttelse af personoplysninger, vedtaget i overensstemmelse med artikel 16 i TEUF.

VEDTAGET FØLGENDE AFGØRELSE:

Artikel 1

Formål

Denne afgørelse regulerer Europa-Parlamentets håndtering og behandling af fortrolige oplysninger, herunder udarbejdelse, modtagelse, fremsendelse og opbevaring af sådanne oplysninger med henblik på at sikre en passende beskyttelse af deres fortrolige karakter. Den gennemfører den interinstitutionelle aftale og Rammeaftalen, særlig dennes bilag II.

Artikel 2

Definitioner

I denne afgørelse finder følgende definitioner anvendelse:

a) Ved »oplysninger« forstås alle skriftlige eller mundtlige oplysninger, uanset medium og udsteder.

b) Ved »fortrolige oplysninger« forstås »klassificerede oplysninger« og ikke-klassificerede »andre fortrolige oplysninger«.

c) Ved »klassificerede oplysninger« forstås »EU-klassificerede oplysninger« og »tilsvarende klassificerede oplysninger«.

d) Ved »EU-klassificerede oplysninger« (»EUCI«) forstås enhver oplysning og ethvert materiale klassificeret som TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED, der ved uberettiget videregivelse i forskellig grad kunne skade Unionens interesser eller en eller flere medlemsstater, uanset om sådanne oplysninger hidrører fra Unionens institutioner, organer, kontorer eller agenturer oprettet med hjemmel i traktaterne eller ej. I den forbindelse er oplysninger og materiale klassificeret på niveau:

— TRÈS SECRET UE/EU TOP SECRET: oplysninger og materiale, hvis uberettigede videregivelse kunne forvolde Unionens eller en eller flere af dens medlemsstaters vitale interesser overordentlig alvorlig skade

— SECRET UE/EU SECRET: oplysninger og materiale, hvis uberettigede videregivelse kunne forvolde Unionens eller en eller flere af dens medlemsstaters vitale interesser alvorlig skade

— CONFIDENTIEL UE/EU CONFIDENTIAL: oplysninger og materiale, hvis uberettigede videregivelse kunne forvolde Unionens eller en eller flere af dens medlemsstaters vitale interesser skade.

— RESTREINT UE/EU RESTRICTED: oplysninger og materiale, hvis uberettigede videregivelse kunne være uhensigtsmæssig for Unionens eller en eller flere af dens medlemsstaters interesser.

e) Ved »tilsvarende klassificerede oplysninger« forstås klassificerede oplysninger, udarbejdet af medlemsstater, tredjelande eller internationale organisationer, som er forsynet med en sikkerhedsklassifikationsmærkning svarende til en af de sikkerhedsklassifikationsmærkninger, der anvendes til EUCI, og som Rådet eller Kommissionen har sendt til Europa-Parlamentet.

f) Ved »andre fortrolige oplysninger« forstås enhver anden form for ikke-klassificerede fortrolige oplysninger, herunder oplysninger, der er omfattet af regler om databeskyttelse eller tavshedspligt, og som er udarbejdet i Europa-Parlamentet, eller som andre institutioner, organer, kontorer og agenturer oprettet med hjemmel i traktaterne eller medlemsstater har sendt til Europa-Parlamentet.

g) Ved »dokument« forstås registrerede informationer uanset deres fysiske form eller karakteristika.

h) Ved »materiale« forstås ethvert dokument eller enhver maskine eller ethvert udstyr, der enten er fremstillet eller er ved at blive fremstillet.

i) Ved »need to know« forstås en bestemt persons behov for at få adgang til fortrolige oplysninger for at kunne varetage sin funktion eller udføre sin opgave.

j) Ved »godkendelse« forstås en beslutning truffet af formanden, hvis den vedrører medlemmer af Europa-Parlamentet, eller af generalsekretæren, hvis den vedrører Europa-Parlamentets tjenestemænd og Europa-Parlamentets øvrige ansatte, der arbejder for politiske grupper, om at give en enkeltperson adgang til klassificerede oplysninger op til et bestemt niveau, efter at en sikkerhedsundersøgelse foretaget af en national myndighed i henhold til den nationale lovgivning og bestemmelserne i bilag I, del 2, har givet et positivt resultat.

k) Ved »nedklassificering« forstås fastsættelse af en lavere klassifikationsgrad end den hidtil gældende.

l) Ved »afklassificering« forstås ophævelse af enhver form for klassificering.

m) Ved »påtegning« forstås et mærke, der er tilføjet på »andre fortrolige oplysninger«, og som har til formål at gøre opmærksom på foruddefinerede specifikke instrukser om dets behandling eller om det område, det pågældende dokument omhandler. Det kan også være tilføjet på klassificerede oplysninger med henblik på at pålægge yderligere krav til behandlingen af disse.

n) Ved »fjernelse af påtegning« forstås fjernelse af enhver form for påtegning.

o) Ved »udsteder« forstås den behørigt bemyndigede ophavsmand til fortrolige oplysninger.

p) Ved »sikkerhedsmeddelelser« forstås tekniske gennemførelsesbestemmelser som fastlagt i bilag II.

q) Ved »behandlingsinstrukser« forstås de tekniske instrukser til Europa-Parlamentets tjenestegrene vedrørende behandling af fortrolige oplysninger.

Artikel 3

Grundlæggende principper og minimumstandarder

1. Europa-Parlamentet behandler fortrolige oplysninger i overensstemmelse med de grundlæggende principper og minimumstandarder, der er fastlagt i bilag I, del 1.

2. Europa-Parlamentet indfører et system til forvaltning af informationssikkerheden i overensstemmelse med de grundlæggende principper og minimumstandarderne. Systemet til forvaltning af informationssikkerheden består af sikkerhedsmeddelelserne, behandlingsinstrukserne og de gældende regler i forretningsordenen. Det har til formål at lette det parlamentariske og administrative arbejde og samtidig sikre, at alle fortrolige oplysninger, der behandles af Europa-Parlamentet, beskyttes i fuld overensstemmelse med de regler, der er fastlagt af udstederen af de pågældende oplysninger i sikkerhedsmeddelelserne.

Europa-Parlamentets behandling af fortrolige oplysninger ved hjælp af automatiske kommunikations- og informationssystemer (CIS) gennemføres i overensstemmelse med begrebet informationssikring som fastsat i sikkerhedsmeddelelse 3.

3. Europa-Parlamentets medlemmer kan få adgang til klassificerede oplysninger op til og med niveauet RESTREINT UE/EU RESTRICTED uden sikkerhedsgodkendelse.

4. Når de pågældende oplysninger er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende, skal der gives adgang hertil for de medlemmer af Europa-Parlamentet, der er godkendt hertil af Europa-Parlamentets formand i henhold til stk. 5, eller efter underskrivelse af en højtidelig erklæring om ikkevideregivelse af indholdet af disse oplysninger til tredjemand, om overholdelse af forpligtelserne til at beskytte oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL og med en bekræftelse på, at vedkommende er bekendt med konsekvenserne af ikke at efterleve dette.

5. Når de pågældende oplysninger er klassificeret på niveau SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, skal der gives adgang hertil for de medlemmer af Europa-Parlamentet, der er godkendt hertil af Europa-Parlamentets formand efter:

a) at de er blevet sikkerhedsgodkendt i overensstemmelse med bilag I, del 2 i denne afgørelse, eller

b) at der er modtaget meddelelse fra en kompetent national myndighed om, at de pågældende medlemmer er behørigt godkendt i kraft af deres funktioner i overensstemmelse med nationale lov.

6. Inden der gives adgang til klassificerede oplysninger, skal medlemmerne af Europa-Parlamentet gøres bekendt med og anerkende deres ansvar for beskyttelse af sådanne oplysninger i overensstemmelse med bilag I. De skal også gøres bekendt med, hvordan denne beskyttelse skal sikres.

7. Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for de politiske grupper, kan få adgang til fortrolige oplysninger, hvis de har »need to know«-status, og kan få adgang til klassificerede oplysninger med en klassificeringsgrad over RESTREINT UE/EU RESTRICTED, hvis de har den fornødne sikkerhedsgodkendelse. Der gives kun adgang til klassificerede oplysninger, hvis de pågældende er blevet gjort bekendt med og har modtaget skriftlige instrukser om deres ansvar for beskyttelse sådanne oplysninger samt om, hvordan denne beskyttelse sikres, og har underskrevet en erklæring som bekræftelse på at have modtaget disse instrukser og på at give tilsagn om at ville overholde dem i overensstemmelse med de eksisterende regler.

Artikel 4

Udarbejdelse af fortrolige oplysninger og Europa-Parlamentets administrative behandling heraf

1. Europa-Parlamentets formand, formændene for de berørte parlamentariske udvalg og generalsekretæren og/eller enhver person, denne har givet behørig skriftlig bemyndigelse hertil, kan oprette fortrolige oplysninger og/eller klassificere oplysninger som beskrevet i sikkerhedsmeddelelserne.

2. Når der oprettes klassificerede oplysninger, anvender udstederen en passende klassificeringsgrad i overensstemmelse med de internationale standarder og definitioner i bilag I. Udstederen bestemmer som hovedregel også, hvilke adressater der skal kunne få adgang til oplysningerne, i forhold til klassificeringsgraden. Disse oplysninger gives til Enheden for Klassificerede Oplysninger (»CIU«), når dokumentet indleveres til CIU.

3. Andre fortrolige oplysninger, der er omfattet af tavshedspligt, behandles i overensstemmelse med instrukserne i bilag I og II og behandlingsinstrukserne.

Artikel 5

Europa-Parlamentets modtagelse af fortrolige oplysninger

1. Fortrolige oplysninger, som Europa-Parlamentet modtager, meddeles som følger:

a) oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og andre fortrolige oplysninger: til sekretariatet for det berørte parlamentariske organ/den hvervsindehaver, der har indgivet anmodningen herom, eller direkte til CIU

b) oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIEL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende: til CIU.

2. Fortrolige oplysningers registrering, opbevaring og sporbarhed behandles af henholdsvis sekretariatet for det parlamentariske organ/den hvervsindehaver, der modtog oplysningerne, eller CIU.

3. De nærmere regler, der fastlægges ved fælles overenskomstmed henblik på at bevare oplysningernes fortrolighed, indleveres i tilfælde af fortrolige oplysninger meddelt af Kommissionen i henhold til punkt 3.2 i bilag II til Rammeaftalen eller i tilfælde af klassificerede oplysninger meddelt af Rådet i henhold til artikel 5, stk. 4 i den interinstitutionelle aftale sammen med de fortrolige oplysninger til henholdsvis sekretariatet for det parlamentariske organ/hvervsindehaveren eller til CIU.

4. De i stk. 3 omhandlede nærmere regler kan også gælde tilsvarende for meddelelse af fortrolige oplysninger, der fremsendes af andre institutioner, organer, kontorer eller agenturer oprettet med hjemmel i traktaterne eller af medlemsstater.

5. Med henblik på at sikre et beskyttelsesniveau, der svarer til klassificering på niveau TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, opretter Formandskonferencen et tilsynsudvalg. Oplysninger klassificeret på niveau TRÈS SECRET UE/EU TOP SECRET eller tilsvarende fremsendes til Europa-Parlamentet i overensstemmelse med yderligere nærmere regler, der aftales mellem Europa-Parlamentet og den EU-institution, som oplysningerne modtages fra.

Artikel 6

Europa-Parlamentets videregivelse af klassificerede oplysninger til tredjemand

Europa-Parlamentet kan, efter forudgående skriftligt samtykke fra udstederen eller den EU-institution, der har fremsendt de klassificerede oplysninger til Europa-Parlamentet, videregive sådanne klassificerede oplysninger til tredjepart på betingelse af, at de sikrer, at regler, der svarer til de i denne afgørelse fastlagte, overholdes inden for deres tjenester og deres bygninger i forbindelse med behandling af disse oplysninger.

Artikel 7

Sikrede faciliteter

1. Europa-Parlamentet etablerer et sikret område og sikre læseværelser til behandling af fortrolige oplysninger.

2. Det sikrede område skal råde over faciliteter til registrering, konsultation, arkivering, overførsel og behandling af klassificerede oplysninger. Det skal bl.a. indeholde et læseværelse og et mødeværelse til konsultation af klassificerede oplysninger og administreres af CIU.

3. Uden for det sikrede område, kan der oprettes sikre læseværelser med henblik på at give mulighed for adgang til oplysninger med klassificering på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og »andre fortrolige oplysninger«. Disse sikre læseværelser administreres af de kompetente tjenestegrene i henholdsvis sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU. De må ikke være udstyret med fotokopimaskiner, telefoner, fax, scanner eller andet teknisk udstyr til reproduktion eller videresendelse af dokumenter.

Artikel 8

Registrering, behandling og opbevaring af fortrolige oplysninger

1. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og »andre fortrolige oplysninger« registreres og opbevares af de kompetente tjenestegrene i sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU, afhængigt af hvem der har modtaget oplysningerne.

2. Følgende betingelser gælder for behandling af oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og andre fortrolige oplysninger:

a) dokumenter indleveres personligt til chefen for sekretariatet, som registrerer dem og kvitterer for modtagelsen

b) dokumenterne opbevares indelåst på sekretariatets ansvar, når de ikke er i brug

c) oplysningerne må under ingen omstændigheder gemmes på et andet medie eller videresendes til en anden person. Sådanne dokumenter må kun kopieres på tilbørligt godkendt udstyr som beskrevet i sikkerhedsmeddelelserne

d) kun personer, der er udpeget af udstederen eller af den EU-institution, der fremsendte oplysningerne til Europa-Parlamentet har adgang til disse i overensstemmelse med de i artikel 4, stk. 2, eller artikel 5, stk. 3, 4 og 5, omtalte nærmere regler

e) sekretariatet for det parlamentariske organ/hvervsindehaveren fører en fortegnelse over de personer, der har konsulteret oplysningerne, og datoen og tidspunktet herfor og sender fortegnelsen til CIU samtidig med, at oplysningerne indleveres til CIU.

3. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIEL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende registreres, behandles og opbevares af CIU på det sikrede område i overensstemmelse med det specifikke klassifikationsniveau og som beskrevet i sikkerhedsmeddelelserne.

4. Ved overtrædelse af reglerne i stk. 1-3 underretter henholdsvis den ansvarlige tjenestemand fra sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU generalsekretæren, der indbringer sagen for formanden, hvis der er tale om et medlem af Europa-Parlamentet.

Artikel 9

Adgang til sikrede faciliteter

1. Adgang til det sikrede område er forbeholdt følgende personer:

a) personer, der i medfør af artikel 3, stk. 4-7, har tilladelse til at konsultere de oplysninger, der opbevares på stedet, og som har indsendt en ansøgning i henhold til artikel 10, stk. 1

b) personer, der i medfør af artikel 4, stk. 1, har tilladelse til at udarbejde klassificerede oplysninger, og som har indsendt en ansøgning i henhold til artikel 10, stk. 1

c) Europa-Parlamentets tjenestemænd i CIU

d) de af Europa-Parlamentets tjenestemænd, der har ansvaret for forvaltningen af Kontoret for Fortrolige Oplysninger

e) de af Europa-Parlamentets tjenestemænd, der er ansvarlige for sikkerhed og brandsikkerhed, i det omfang det er nødvendigt.

f) rengøringspersonale, dog kun under tilstedeværelse af og under tæt overvågning af en tjenestemand fra CIU.

2. CIU kan nægte enhver person, der ikke er godkendt dertil, adgang til det sikrede område. Enhver indsigelse mod en sådan nægtelse af adgang indbringes for formanden, når der er tale om anmodninger om adgang fra medlemmer af Europa-Parlamentet, og for generalsekretæren i andre tilfælde.

3. Generalsekretæren kan give tilladelse til et møde for et begrænset antal personer i mødeværelset placeret i det sikrede område.

4. Adgang til et sikkert læseværelse er forbeholdt følgende personer:

a) medlemmer af Europa-Parlamentet, Europa-Parlamentets tjenestemænd og Europa-Parlamentets øvrige ansatte, der arbejder for politiske grupper, som er behørigt identificeret som personer, der har ret til at konsultere eller udarbejde fortrolige oplysninger.

b) de af Europa-Parlamentets tjenestemænd, der har ansvar for forvaltningen af Kontoret for Fortrolige Oplysninger, tjenestemænd fra sekretariatet for det parlamentariske organ/hvervsindehaveren, som har modtaget oplysningerne og tjenestemænd fra CIU

c) i det omfang det er nødvendigt, de af Europa-Parlamentets tjenestemænd, der er ansvarlige for sikkerhed og brandsikkerhed

d) rengøringspersonale, dog kun under tilstedeværelse af og under tæt overvågning af en tjenestemand fra henholdsvis sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU.

5. Henholdsvis det kompetente sekretariat for det parlamentariske organ/hvervsindehaveren eller CIU kan nægte enhver person, der ikke er godkendt dertil, adgang til et sikkert læseværelse. Enhver indsigelse mod en sådan nægtelse indbringes for formanden, når der er tale om anmodninger om adgang fra medlemmer af Europa-Parlamentet, og for generalsekretæren i andre tilfælde.

Artikel 10

Konsultation eller udarbejdelse af fortrolige oplysninger i sikrede faciliteter

1. En person, der ønsker at konsultere eller udarbejde fortrolige oplysninger, meddeler på forhånd sit navn til CIU. CIU kontrollerer identiteten af denne person og undersøger, om den pågældende er godkendt til at konsultere eller udarbejde fortrolige oplysninger, i overensstemmelse med artikel 3, stk. 3-7, artikel 4, stk. 1 eller artikel 5, stk. 3, 4 og 5.

2. En person, der i overensstemmelse med artikel 3, stk. 3 og 7, ønsker at konsultere fortrolige oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende eller »andre fortrolige oplysninger« i et sikkert læseværelse, meddeler på forhånd sit navn til de kompetente tjenestegrene i sekretariaterne for det parlamentariske organ/hvervsindehaveren eller CIU.

3. Bortset fra særlige tilfælde (f.eks. når et stort antal anmodninger er indgivet i løbet af kort tid) må kun én person ad gangen i nærværelse af en tjenestemand fra sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU konsultere fortrolige oplysninger i en sikret facilitet.

4. Under konsultationen er det forbudt at have kontakt med omverdenen (herunder ved brug af telefon eller andre teknologiske indretninger), at tage noter eller at fotokopiere eller fotografere de konsulterede fortrolige oplysninger.

5. Før en person får tilladelse til at forlade den sikre facilitet, kontrollerer tjenestemanden fra sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU, at de konsulterede fortrolige oplysninger stadig er til stede, intakte og fuldstændige.

6. Ved overtrædelse af ovenstående regler underretter den ansvarlige tjenestemand fra sekretariatet for det parlamentariske organ/hvervsindehaveren eller CIU generalsekretæren, der indbringer sagen for formanden, såfremt der er tale om et medlem af Europa-Parlamentet.

Artikel 11

Minimumsstandarder for andre former for konsultation af fortrolige oplysninger i et møde for lukkede døre uden for sikrede faciliteter

1. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og »andre fortrolige oplysninger« kan konsulteres af medlemmer af de parlamentariske udvalg eller af andre politiske og administrative organer i Europa-Parlamentet på et møde for lukkede døre uden for de sikrede faciliteter.

2. I tilfælde som omhandlet i stk. 1 sikrer sekretariatet for det parlamentariske organ/den hvervsindehaver, der er ansvarlig(t) for mødet, at følgende betingelser overholdes:

a) kun de personer, der er udpeget af formanden af det kompetente udvalg eller organ til at deltage i mødet, får adgang til mødeværelset

b) alle dokumenter er nummererede og bliver omdelt ved mødets begyndelse og indsamlet igen ved dets afslutning, og der tages ikke noter eller fotokopier eller fotos af dokumenterne

c) protokollen fra mødet omtaler ikke drøftelsen af de oplysninger, som er blevet behandlet; kun en eventuel relevant afgørelse kan nævnes i protokollen

d) fortrolige oplysninger, som afgives mundtligt til modtagere i Europa-Parlamentet, er omfattet af et beskyttelsesniveau som det eller svarende til det, der ville finde anvendelse for skriftlige fortrolige oplysninger.

e) ingen yderligere samling af dokumenter opbevares i mødeværelser

f) kopier af dokumenter udleveres kun i det nødvendige antal til mødedeltagere og tolke ved mødets begyndelse

g) mødeformanden gør klart fra mødets begyndelse, hvilken status dokumenterne har for så vidt angår klassifikation og påtegning

h) deltagerne fjerner ikke dokumenter fra mødeværelset

i) sekretariatet for det parlamentariske organ/hvervsindehaveren indsamler og står til regnskab for alle kopier af dokumenter ved mødets afslutning

j) der medbringes ingen elektroniske kommunikationsmidler eller andre elektroniske indretninger i mødeværelset, hvor de pågældende fortrolige oplysninger konsulteres eller drøftes.

3. Hvis oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende drøftes på et møde for lukkede døre, i overensstemmelse med undtagelserne i punkt 3.2.2 i bilag II til rammeaftalen og i artikel 6, stk. 5, i den interinstitutionelle aftale, sikrer sekretariatet for det parlamentariske organ/hvervsindehaveren, der er ansvarlig for mødet, i tillæg til sikring af overholdelse af bestemmelserne i stk. 2, at de personer, der er udpeget til at deltage i mødet, opfylder kravene i artikel 3, stk. 4 og 7.

4. I tilfælde som omhandlet i stk. 3 forsyner CIU sekretariatet for det parlamentariske organ/hvervsindehaveren, der er ansvarlig(t) for mødet for lukkede døre, med det fornødne antal kopier af de dokumenter, der skal drøftes, som skal returneres til CIU efter mødet.

Artikel 12

Arkivering af fortrolige oplysninger

1. Der føres et sikkert arkiveringssystem inden for det sikrede område. CIU er ansvarlig for forvaltningen af det sikre arkiv i overensstemmelse med standardkriterier for arkivering.

2. Klassificerede oplysninger, der deponeres endeligt hos CIU, og oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende, der deponeres hos det parlamentariske organs sekretariat/hvervsindehaveren, overføres til det sikre arkiv i det sikrede område seks måneder efter den sidste konsultation og senest et år efter deponeringen. »Andre fortrolige oplysninger« arkiveres af sekretariaterne for de berørte parlamentariske organer/hvervsindehaveren i overensstemmelse med generelle regler om dokumenthåndtering, med mindre de deponeres hos CIU.

3. De fortrolige oplysninger i de sikre arkiver kan konsulteres på følgende betingelser:

a) der gives kun tilladelse til personer, der er identificeret ved navn, funktion eller stilling i det ledsagedokument, der blev udfyldt ved deponering af de fortrolige oplysninger

b) der skal indgives en anmodning om konsultation til CIU, der sørger for overførsel af dokumentet fra arkivet til det sikre læseværelse

c) procedurerne og betingelserne for konsultation af fortrolige oplysninger som fastsat i artikel 10 finder anvendelse.

Artikel 13

Nedklassificering og afklassificering af samt fjernelse af påtegninger på fortrolige oplysninger

1. Fortrolige oplysninger må kun nedklassificeres, afklassificeres eller få fjernet påtegningen efter forudgående tilladelse fra udstederen og om nødvendigt efter drøftelse med andre berørte parter.

2. Nedklassificeringen eller afklassificeringen bekræftes skriftligt. Udstederen er ansvarlig for at underrette modtagerne om ændringen, og disse er på deres side ansvarlige for at underrette efterfølgende modtagere, til hvem de har sendt eller kopieret dokumentet, om ændringen. Så vidt muligt anfører udstederen på de klassificerede dokumenter en dato, periode eller begivenhed, efter hvilken indholdet kan nedklassificeres eller afklassificeres. I modsat fald skal vedkommende tage klassificeringen op til revision mindst hvert femte år for at undersøge, om den oprindelige klassifikationsgrad stadig er nødvendig.

3. Fortrolige oplysninger i de sikre arkiver undersøges i god tid, og senest på dagen 25 år efter deres udarbejdelse, med henblik på at fastslå, om de bør afklassificeres, nedklassificeres eller have fjernet påtegningen. Undersøgelse og offentliggørelse af sådanne oplysninger finder sted i overensstemmelse med bestemmelserne i 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 ([1]). Afklassificeringen foretages af udstederen til de klassificerede oplysninger eller af det på det relevante tidspunkt ansvarlige kontor i overensstemmelse med bilag I, del 1, punkt 10.

4. Efter nedklassificering overføres tidligere klassificerede oplysninger, der opbevares i det sikre arkiv, til Europa-Parlamentets historiske arkiver til permanent bevaring og videre behandling i overensstemmelse med de gældende regler.

5. Efter fjernelse af en påtegning, er oplysninger, der tidligere var mærket »andre fortrolige oplysninger«, underlagt Europa-Parlamentets regler om dokumenthåndtering.

Artikel 14

Brud på sikkerheden, tab eller kompromittering af fortrolige oplysninger

1. Et brud på fortroligheden i almindelighed og på disse regler i særdeleshed fører, når der er tale om medlemmer af Europa-Parlamentet, til anvendelse af de relevante bestemmelser om sanktioner i Europa-Parlamentets forretningsorden.

2. Et brud på reglerne begået af en af Europa-Parlamentets ansatte fører til anvendelse af procedurerne og sanktionerne i henholdsvis vedtægten for tjenestemænd og ansættelsesvilkårene for de øvrige ansatte i Den europæiske Union, fastlagt i Forordning (EØF, Euratom, EKSF) nr. 259/68 ([2]) (»personalevedtægterne«).

([1]) EFT L 43 af 15.2.1983, s. 1.
([2]) EFT L 56 af 4.3.1968, s. 1.

3. Formanden og/eller generalsekretæren, afhængigt af den konkrete situation, iværksætter de nødvendige undersøgelser i tilfælde af et brud som defineret i sikkerhedsmeddelelse 6.

4. Hvis de fortrolige oplysninger blev meddelt Europa-Parlamentet af en anden EU-institution eller af en medlemsstat, underretter formanden og/eller generalsekretæren, afhængigt af det konkrete tilfælde, den pågældende EU-institution eller medlemsstat om eventuelle beviste eller formodede tab eller kompromitteringer af klassificerede oplysninger, om resultaterne af undersøgelsen og om de foranstaltninger, der træffes for at forebygge en gentagelse.

Artikel 15

Tilpasning af denne afgørelse og gennemførelsesbestemmelserne hertil og årsberetning om anvendelsen af denne afgørelse

1. Generalsekretæren foreslår de nødvendige tilpasninger af denne afgørelse og gennemførelsesbestemmelserne i bilagene og forelægger forslagene for Præsidiet til afgørelse.

2. Generaldirektøren er ansvarlig for Europa-Parlamentets tjenestegrenes gennemførelse af denne afgørelse og udsteder behandlingsinstrukser om anliggender, der er omfattet af systemet til forvaltning af informationssikkerheden i overensstemmelse med principperne i denne beslutning.

3. Generalsekretæren forelægger en årsberetning for Præsidiet om anvendelsen af denne afgørelse.

Artikel 16

Gældende bestemmelser og overgangsbestemmelser

1. Ikke-klassificerede oplysninger, der opbevaredes i CIU eller i ethvert andet af Europa-Parlamentets arkiver, og som betragtes som fortrolige og er dateret før 1. april 2014, anses i denne afgørelse for at udgøre »andre fortrolige oplysninger«. Udstederen heraf kan når som helst beslutte at ændre oplysningernes fortrolighedsniveau.

2. Uanset artikel 5, stk. 1, litra a), og artikel 8, stk. 1, i denne afgørelse skal oplysninger, der meddeles fra Rådet i overensstemmelse med den interinstitutionelle aftale, og som er klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende, deponeres hos, registreres af og opbevares i CIU i en periode på tolv måneder fra 1. april 2014. Disse oplysninger kan konsulteres i overensstemmelse med artikel 4, stk. 2, litra a) og c), og artikel 5, stk. 4, i den interinstitutionelle aftale.

3. Præsidiets afgørelse af 6. juni 2011 om regler om Europa-Parlamentets behandling af fortrolige oplysninger ophæves.

Artikel 17

Ikrafttræden

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

BILAG I

Del 1

GRUNDLÆGGENDE PRINCIPPER OG MINIMUMSSTANDARDER FOR SIKKERHED I FORBINDELSE MED BESKYTTELSE AF FORTROLIGE OPLYSNINGER

1. **INDLEDNING**

I disse forskrifter fastlægges de grundlæggende principper og minimumssikkerhedsstandarder for beskyttelse af fortrolige oplysninger, som skal følges og/eller overholdes af Europa-Parlamentet på alle dets tjenestesteder, herunder af alle modtagere af klassificerede oplysninger og »andre fortrolige oplysninger«, for at værne om sikkerheden og for at sikre alle berørte, at der gælder en fælles standard for sikkerhedsbeskyttelse. Disse bestemmelser suppleres af sikkerhedsmeddelelserne i bilag II og andre bestemmelser om parlamentsudvalgs og andre parlamentsorganers/hvervsindehaveres behandling af fortrolige oplysninger.

2. **GENERELLE PRINCIPPER**

Europa-Parlamentets sikkerhedspolitik indgår som en integrerende del af dets almindelige interne forvaltningspolitik og er dermed baseret på de principper, der gælder for denne almindelige politik. Disse principper omfatter bl.a. legalitet, åbenhed, ansvarlighed, samt subsidiaritet og proportionalitet.

Legalitet medfører, at de gældende rammebestemmelser nøje skal iagttages ved udøvelsen af sikkerhedsfunktionerne, og at alle de krav i bestemmelserne, der finder anvendelse, skal opfyldes. Endvidere skal ansvar på områderne vedrørende sikkerhed have hjemmel i gældende bestemmelser. Personalevedtægternes bestemmelser, navnlig artikel 17 om personalets forpligtelse til at afholde sig fra enhver uberettiget afsløring af oplysninger, som han har fået kendskab til i forbindelse med udøvelsen af sit arbejde, og afsnit VI om disciplinærordningen, finder fuld anvendelse. Endelig behandles brud på sikkerhedsbestemmelserne inden for Europa-Parlamentets ansvarsområde i overensstemmelse dets forretningsorden og med dets politik vedrørende disciplinære sanktioner.

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

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

Subsidiaritet betyder, at sikkerheden skal tilrettelægges på det lavest mulige niveau og så nært på Europa-Parlamentets generaldirektorater og tjenestegrene som muligt.

Proportionalitet betyder, at sikkerhedsaktiviteterne nøje skal begrænses til det absolut nødvendige, og at sikkerhedsforanstaltningerne skal stå i forhold til de interesser, der skal beskyttes, og til den faktiske eller potentielle trussel mod disse interesser, så interesserne kan forsvares på en måde, der sikrer mindst mulige forstyrrelser.

3. **GRUNDLAGET FOR SIKKERHEDSBESKYTTELSE AF OPLYSNINGER**

Grundlaget for en effektiv sikkerhedsbeskyttelse af oplysninger er:

a) egnede kommunikations- og informationssystemer (CIS). Disse falder ind under Europa-Parlamentets sikkerhedsmyndigheds ansvar (som defineret i sikkerhedsmeddelelse 1)

b) at der i Parlamentet udpeges en informationssikringsmyndighed (som defineret i sikkerhedsmeddelelse 1), som inden for den pågældende sikkerhedsmyndighed er ansvarlig for at underrette og rådgive om tekniske sikkerhedsrisici i forhold til CIS og modforholdsregler mod disse trusler

c) at der er nært samarbejde mellem Europa-Parlamentets ansvarlige tjenester og sikkerhedstjenesterne ved de øvrige EU-institutioner.

4. **PRINCIPPERNE FOR INFORMATIONSSIKKERHED**

4.1. ***Formål***

Informationssikkerhedens vigtigste formål er:

a) at beskytte fortrolige oplysninger mod spionage, kompromittering eller uautoriseret videregivelse

b) at beskytte klassificerede oplysninger, der behandles i kommunikations- og informationssystemer og -netværk, mod trusler imod deres fortrolighed, integritet og tilgængelighed

c) at beskytte Europa-Parlamentets bygninger, der rummer klassificerede oplysninger, mod sabotage, hærværk og anden forsætlig skade

d) i tilfælde af brud på sikkerhedsforskrifterne at vurdere den forvoldte skade, begrænse følgerne, foretage sikkerhedsmæssig efterforskning og træffe eventuelle nødvendige afhjælpende foranstaltninger.

4.2. ***Klassifikation***

4.2.1. Der skal udvises stor omhu og eftertanke ved udvælgelsen af, hvilke oplysninger og hvilket materiale der skal beskyttes, og ved vurderingen af, hvilken grad af beskyttelse der er behov for. Det er afgørende, at beskyttelsesgraden stemmer overens med den sikkerhedsmæssige følsomhed, som for den enkelte oplysning eller det enkelte materiale skal beskyttes. For at sikre en smidig informationsstrøm skal det undgås, at der anvendes en for høj eller for lav klassifikationsgrad.

4.2.2. Klassificeringsordningen er det instrument, hvormed principperne i dette punkt gennemføres; der anvendes en tilsvarende klassificeringsordning ved planlægning og tilrettelæggelse af beskyttelsen mod spionage, sabotage, terrorisme og andre trusler, for at sikre, at de vigtigste bygninger og områder, der rummer klassificerede oplysninger, og de mest følsomme steder i disse bygninger og områder sikres bedst.

4.2.3. Ansvaret for klassificering af oplysninger påhviler alene udstederen af de pågældende oplysninger.

4.2.4. Klassifikationsgraden baseres alene på indholdet af de pågældende oplysninger.

4.2.5. Flere dokumenter med oplysninger, der er grupperet sammen, skal klassificeres mindst lige så højt som det højeste af de enkelte dokumenters klassifikationsniveauer. Dog kan en samling af oplysninger kan dog tildeles et højere klassifikationsniveau end de enkelte dele.

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

4.3. ***Sikkerhedsforanstaltningernes formål***

Sikkerhedsforanstaltningerne skal:

a) omfatte alle personer med adgang til klassificerede oplysninger, medier med klassificerede oplysninger og »andre fortrolige oplysninger«, såvel som alle bygninger og områder, der rummer sådanne oplysninger, og vigtige anlæg

b) udformes, så de identificerer personer, som (i kraft af adgang, kontakter eller på anden måde) kan udgøre en sikkerhedsmæssig risiko for sådanne oplysninger og for vigtige anlæg, der rummer sådanne oplysninger, og enten forhindre, at de får adgang hertil, eller sørge for, at de flyttes fra det pågældende sted

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

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

e) sikre alle fortrolige oplysningers integritet (ved at hindre forvanskning eller uautoriseret ændring eller uautoriseret slettelse) og tilgængelighed (for autoriserede brugere, når de skal anvendes), navnlig oplysninger, som lagres, behandles eller fremsendes elektronisk.

5. FÆLLES MINIMUMSSTANDARDER

Europa-Parlamentet sikrer, at alle modtagere af klassificerede oplysninger, såvel i institutionen som under dens kompetenceområde, dvs. alle tjenestegrene og leverandører, overholder fælles minimumsstandarder for sikkerhed, så sådanne oplysninger kan videregives i tillid til, at de vil blive sikret på passende vis. Disse minimumsstandarder skal omfatte kriterier for sikkerhedsgodkendelse af Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper, samt procedurer for beskyttelse af fortrolige oplysninger.

Europa-Parlamentet giver kun tredjepart adgang til sådanne oplysninger, hvis denne tredjepart garanterer, at der ved behandlingen af oplysningerne iagttages bestemmelser, der som minimum nøje svarer til disse fælles minimumsstandarder.

Sådanne fælles minimumsstandarder anvendes også, når Europa-Parlamentet overdrager opgaver, som involverer fortrolige oplysninger, til erhvervsmæssige eller andre eksterne enheder ved kontrakt eller tilskudsaftale.

6. SIKKERHEDSFORANSTALTNINGER VEDRØRENDE EUROPA-PARLAMENTETS TJENESTEMÆND OG PARLAMENTETS ØVRIGE ANSATTE, DER ARBEJDER FOR POLITISKE GRUPPER

6.1. *Sikkerhedsinstrukser vedrørende Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper*

For Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper, gælder, at de, der varetager opgaver, hvor de kan få adgang til klassificerede oplysninger, inden de påbegynder arbejdet og derefter regelmæssigt, skal modtage en indgående instruks om nødvendigheden af sikkerhedsbeskyttelsen og de procedurer dette omfatter. Sådanne personer skal skriftligt bekræfte, at de har læst og fuldt ud forstået de sikkerhedsbestemmelser, der finder anvendelse.

6.2. *Ledelsens ansvar*

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

6.3. *Sikkerhedsstatus for Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper*

Der indføres procedurer for at sikre, at der, hvis der fremkommer negative oplysninger om en af Europa-Parlamentets tjenestemænd eller af Parlamentets øvrige ansatte, der arbejder for en politisk gruppe, bliver taget skridt til at fastslå, om den pågældende i sit arbejde behandler klassificerede oplysninger, eller om den pågældende har adgang til sikre kommunikations- og informationssystemer, og at Europa-Parlamentets kompetente tjeneste underrettes. Hvis den kompetente nationale sikkerhedsmyndighed indikerer, at medarbejderen udgør en sikkerhedsrisiko, skal den pågældende udelukkes fra eller fratages arbejdsopgaver, hvor vedkommende kan være til fare for sikkerheden.

7. FYSISK SIKKERHED

Fysisk sikkerhed indebærer anvendelse af fysiske og tekniske beskyttelsesforanstaltninger til at forhindre uautoriseret adgang til klassificerede oplysninger.

7.1. ***Behovet for sikkerhedsbeskyttelse***

Graden af de fysiske foranstaltninger, der skal bringes i anvendelse for at sikre beskyttelsen af klassificerede oplysninger, skal stå i forhold til klassifikationsgraden samt omfanget af og truslen mod de oplysninger og det materiale, det drejer sig om. Alle, der ligger inde med klassificerede oplysninger, skal følge en ensartet praksis med hensyn til klassificering af sådanne oplysninger og opfylde fælles standarder for sikkerhedsbeskyttelse for så vidt angår opbevaring, fremsendelse og bortskaffelse af oplysninger og materiale, der skal beskyttes.

7.2. ***Kontrol***

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

7.3. ***Sikkerhedsbeskyttelse af bygninger***

Bygninger, der rummer klassificerede oplysninger eller sikre kommunikations- og informationssystemer, skal beskyttes mod uautoriseret adgang.

Hvordan klassificerede oplysninger skal beskyttes, med gitre for vinduer, låse på døre, vagtposter ved indgange, automatiske adgangskontrolsystemer, sikkerhedskontrol og -patruljering, alarm- og overvågningssystemer, vagthunde m.v., afhænger af:

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

b) kvaliteten af de sikre skabe eller bokse, hvor oplysningerne eller materialet opbevares, og

c) bygningens fysiske beskaffenhed og beliggenhed.

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

7.4. ***Beredskabsplaner***

Der skal på forhånd foreligge detaljerede planer til sikring af beskyttelsen af klassificerede oplysninger, hvis der opstår en kritisk situation.

8. **SIKKERHEDSANGIVELSER, PÅTEGNINGER, ANFØRELSE OG KLASSIFIKATIONSSTYRING**

8.1. ***Sikkerhedsangivelser***

Der må ikke anvendes andre klassifikationsgrader end dem, der er fastlagt i denne afgørelses artikel 2, litra d).

Til begrænsning af gyldighedsperioden for en klassifikationsgrad (angivelse af automatisk nedklassificering eller afklassificering af klassificerede oplysninger) kan der benyttes en godkendt sikkerhedsangivelse.

Sikkerhedsangivelser må kun benyttes i forbindelse med en klassifikationsgrad.

Sikkerhedsangivelser reguleres yderligere i sikkerhedsmeddelelse 2 og defineres i behandlingsinstrukserne.

8.2. ***Påtegninger***

En påtegning bruges til at angive foruddefinerede specifikke instruktioner om behandlingen af fortrolige oplysninger. Med påtegninger kan også angives, hvilket område et dokument omhandler, hvordan det skal fordeles efter »need to know«-princippet, eller hvornår en embargo ophører (for ikke-klassificerede oplysninger).

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

Påtegninger reguleres yderligere i sikkerhedsmeddelelse 2 og defineres i behandlingsinstrukserne.

8.3. ***Anførelse af klassifikationsgrad og sikkerhedspåtegninger***

Anførelse af klassifikationsgrad, sikkerhedspåtegninger og andre påtegninger foretages i overensstemmelse med sikkerhedsmeddelelse 2, afsnit E og behandlingsinstrukserne.

8.4. ***Klassifikationsstyring***

8.4.1 *Generelt*

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

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

Europa-Parlamentets tjenestemænd klassificerer, nedklassificerer eller afklassificerer oplysninger efter instruks fra eller med beføjelse fra generalsekretæren.

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

Antallet af medarbejdere, der har bemyndigelse til at udstede klassificerede oplysninger med klassifikationsniveauet TRÈS SECRET UE/EU TOP SECRET, skal holdes på et minimum, og deres navne skal opføres på en liste, der udarbejdes af CIU.

8.4.2 *Anvendelse af klassifikationsgrader*

Klassificeringen af et dokument afhænger af, hvor følsomt dets indhold er, jf. definitionen i artikel 2, litra d). Det er vigtigt, at oplysninger klassificeres korrekt og at der ikke anvendes en for høj klassifikationsgrad.

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

Udstederen skal ved klassificeringen af et dokument følge ovenstående bestemmelser og undgå enhver form for over- eller underklassifikation.

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

9. **INSPEKTION**

Europa-Parlamentets Direktorat for Sikkerhed og Risikovurdering gennemfører regelmæssige interne inspektioner af sikkerhedsordningerne til beskyttelse af klassificerede oplysninger og kan i denne forbindelse anmode om bistand fra Rådets eller Kommissions sikkerhedsmyndigheder.

EU-institutionernes sikkerhedsmyndigheder og kompetente tjenestegrene kan som led i en aftalt proces på foranledning af den ene eller den anden part gennemføre peer-evalueringer af sikkerhedsordningerne for beskyttelse af klassificerede oplysninger, der udveksles under de relevante interinstitutionelle aftaler.

10. **PROCEDURER FOR AFKLASSIFICERING OG FJERNELSE AF PÅTEGNINGER**

10.1. CIU gennemgår de fortrolige oplysninger, der er indeholdt i dets register og anmoder om tilsagn fra udstederen af et dokument til at afklassificere eller fjerne påtegningerne på dette senest på dagen 25 år efter datoen for dets udarbejdelse. Dokumenter, der ikke er blevet afklassificeret eller har fået fjernet påtegningerne ved første gennemgang, gennemgås igen regelmæssigt og mindst hvert femte år. Udover at finde anvendelse for dokumenter, der faktisk befinder sig i de sikre arkiver i det sikrede område og er blevet behørigt klassificeret, kan proceduren for fjernelse af påtegninger endvidere finde anvendelse på andre fortrolige oplysninger, der opbevares enten hos Parlaments tjenestegrene eller hos de tjenestegrene, der har ansvaret for Parlamentets historiske arkiver.

10.2 Beslutningen om at afklassificere eller fjerne påtegningerne på et dokument træffes som hovedregel udelukkende af udstederen, eller undtagelsesvis i samarbejde med den af Parlamentets tjenestegrene, der opbevarer dette, inden de oplysninger, det indeholder, overføres til den tjenestegren, der har ansvaret for Parlamentets historiske arkiver. Afklassificering eller fjernelse af påtegninger på klassificerede oplysninger kan kun finde sted efter forudgående skriftligt samtykke fra udstederen. Hvis der er tale om »andre fortrolige oplysninger«, beslutter sekretariatet for den tjenestegren i Parlamentet, der opbevarer disse oplysninger, i samarbejde med udstederen, hvorvidt påtegningerne på dokumentet kan fjernes.

10.3. På vegne af udstederen er CIU ansvarlig for at underrette dokumentets modtagere om ændringen af klassificeringen eller påtegningen, og disse er på deres side ansvarlige for at underrette efterfølgende modtagere, til hvem de har sendt eller kopieret dokumentet.

10.4. Afklassificeringen berører ikke eventuelle sikkerhedspåtegninger eller andre påtegninger på dokumentet.

10.5. I tilfælde af afklassificering overstreges den oprindelige klassifikation for oven og for neden på hver enkelt side. Dokumentets første side stemples og forsynes med CIUs reference. I tilfælde af fjernelse af påtegninger overstreges den oprindelige påtegning for oven på hver enkelt side.

10.6. Teksten fra det dokument, der er blevet afklassificeret eller har fået fjernet påtegningerne, vedhæftes den elektroniske fil eller det tilsvarende system, hvori det er blevet registreret.

10.7. Med hensyn til dokumenter, der er omfattet af undtagelserne vedrørende privatlivets fred og den enkeltes integritet eller en fysisk eller juridisk persons forretningsmæssige interesser, og i tilfælde af følsomme dokumenter finder bestemmelserne i artikel 2 i forordning (EØF, Euratom) nr. 354/83 anvendelse.

10.8. I tillæg til bestemmelserne i punkt 10.1 til 10.7 gælder følgende:

a) Med hensyn til dokumenter fra tredjemand rådfører CIU sig med den pågældende tredjemand, før det iværksætter en afklassificering eller fjernelse af påtegninger.

b) For så vidt angår undtagelsen vedrørende privatlivets fred og den enkeltes integritet tages ved en procedure for afklassificering eller fjernelse af påtegninger navnlig hensyn til, at den berørte har givet samtykke, eller at det i påkommende tilfælde er umuligt at identificere den berørte person.

c) For så vidt angår undtagelsen vedrørende en fysisk eller juridisk persons forretningsmæssige interesser kan den pågældende person eventuelt gives meddelelse ved offentliggørelse i *Den Europæiske Unions Tidende* sammen med en tidsfrist på fire uger efter datoen for denne offentliggørelse til at fremsætte eventuelle bemærkninger.

Del 2

SIKKERHEDSGODKENDELSE

11. **SIKKERHEDSGODKENDELSE AF MEDLEMMER AF EUROPA-PARLAMENTET**

11.1. For at få adgang til oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende skal medlemmer af Europa-Parlamentet først godkendes til den pågældende klassifikationsgrad enten efter proceduren i punkt 11.3 og 11.4 i nærværende bilag eller på grundlag af en højtidelig erklæring om ikkevideregivelse i henhold til artikel 3, stk. 4. i denne afgørelse.

11.2 For at få adgang til oplysninger klassificeret på niveau SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende skal medlemmerne af Europa-Parlamentet først godkendes til den pågældende klassifikationsgrad efter proceduren i punkt 11.3 og 11.14.

11.3. Kun de af Europa-Parlamentets medlemmer, der er blevet sikkerhedsundersøgt af medlemsstaternes kompetente nationale myndigheder (den nationale sikkerhedsmyndighed) efter proceduren i punkt 11.9 til 11.14, kan godkendes. Formanden er ansvarlig for at give godkendelse af medlemmer.

11.4 Formanden kan meddele skriftlig godkendelse efter at have indhentet udtalelse fra medlemsstaternes nationale myndigheder på grundlag af den sikkerhedsundersøgelse, der er foretaget i henhold til punkt 11.8 til 11.13.

11.5. Europa-Parlamentets Direktorat for Sikkerhed og Risikovurdering ajourfører løbende en liste over alle de af Europa-Parlamentets medlemmer, der har fået godkendelse, herunder midlertidig godkendelse som omhandlet i punkt 11.15.

11.6. Godkendelsen er gyldig i fem år eller i varigheden af de arbejdsopgaver, der ligger til grund for den, idet den korteste af disse perioder finder anvendelse. Godkendelsen kan fornys efter proceduren i punkt 11.4.

11.7. Formanden inddrager godkendelsen, hvis vedkommende finder, at der er grund til sådan inddragelse. Inddrages godkendelsen, underrettes det pågældende medlem af Europa-Parlamentet, der kan anmode om at måtte fremsætte sine bemærkninger over for formanden, inden inddragelsen får virkning, samt de nationale myndigheder.

11.8. Sikkerhedsundersøgelsen foretages med det berørte Europa-Parlamentsmedlems medvirken og efter anmodning fra formanden. Den for sikkerhedsundersøgelsen kompetente nationale myndighed er myndigheden i den medlemsstat, hvor det pågældende medlem er statsborger.

11.9. Det pågældende medlem af Europa-Parlamentet skal som led i sikkerhedsundersøgelsen udfylde et skema med angivelse af personlige oplysninger.

11.10. Formanden giver i sin anmodning til den kompetente nationale myndighed nærmere oplysninger om arten af og klassifikationsgraden for de oplysninger, som det pågældende medlem af Europa-Parlamentet vil få kendskab til, så den kan foretage sikkerhedsundersøgelsen.

11.11 De bestemmelser om sikkerhedsundersøgelse, som er gældende i den berørte medlemsstat, herunder bestemmelser om eventuel klageadgang, finder anvendelse i forbindelse med hele den af den kompetente nationale myndighed foretagne sikkerhedsundersøgelses forløb og dens resultater.

11.12. Afgiver den kompetente nationale myndighed positiv udtalelse, kan formanden godkende det pågældende medlem af Europa-Parlamentet.

11.13. Afgiver den kompetente nationale myndighed negativ udtalelse, underrettes det pågældende medlem af Europa-Parlamentet, der kan anmode om at måtte fremsætte sine bemærkninger over for formanden. Hvis formanden finder det nødvendigt, kan den pågældende rette henvendelse til den kompetente nationale myndighed og bede om eventuelle yderligere oplysninger. Bekræftes den negative udtalelse, kan der ikke meddeles godkendelse.

11.14. Ethvert medlem af Europa-Parlamentet, der godkendes efter punkt 11.3, får i forbindelse med godkendelsen og siden med jævne mellemrum de nødvendige retningslinjer for beskyttelse af klassificerede oplysninger og om, hvordan de skal beskyttes. Sådanne medlemmer underskriver en erklæring som bekræftelse på at have modtaget disse retningslinjer.

11.15. Formanden kan undtagelsesvis meddele midlertidig godkendelse af et medlem af Europa-Parlamentet for et tidsrum på højst seks måneder, mens resultatet af sikkerhedsundersøgelsen som omhandlet i punkt 11.11 afventes, forudsat at den kompetente nationale myndighed på forhånd er blevet underrettet, og der ikke er modtaget bemærkninger herfra inden for en måned. Midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret på niveau TRÈS SECRET UE/EU TOP SECRET eller tilsvarende.

12. SIKKERHEDSGODKENDELSE AF EUROPA-PARLAMENTETS TJENESTEMÆND OG PARLAMENTETS ØVRIGE ANSATTE, DER ARBEJDER FOR POLITISKE GRUPPER

12.1. Kun Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper, og som i embeds medfør og af tjenstlige grunde har brug for at få kendskab til eller behandle klassificerede oplysninger, har adgang hertil.

12.2. For at få adgang til oplysninger, der er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, skal de pågældende tjenestemænd i Europa-Parlamentet og øvrige ansatte, der arbejder for berørte politiske grupper først godkendes til den pågældende klassifikationsgrad efter proceduren i punkt 12.3 og 12.4.

12.3. Kun personer som omhandlet i punkt 12.1, der er blevet sikkerhedsundersøgt af medlemsstaternes nationale myndigheder (den nationale sikkerhedsmyndighed) efter proceduren i punkt 12.9 til 12.14, kan godkendes. Generalsekretæren er ansvarlig for at give godkendelse af Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper.

12.4. Generalsekretæren kan meddele skriftlig godkendelse efter at have indhentet udtalelse fra medlemsstaternes kompetente nationale myndigheder på grundlag af den sikkerhedsundersøgelse, der er foretaget i overensstemmelse med punkt 12.8 til 12.13.

12.5. Europa-Parlamentets Direktorat for Sikkerhed og Risikovurdering ajourfører løbende en liste over alle stillinger, der kræver sikkerhedsgodkendelse, som Europa-Parlamentets tjenestegrene har angivet, og over alle medarbejdere, der har fået godkendelse, herunder midlertidig godkendelse i den i punkt 12.15 anvendte betydning.

12.6. Godkendelsen er gyldig i fem år eller i varigheden af de arbejdsopgaver, der ligger til grund for den, idet den korteste af disse perioder finder anvendelse. Godkendelsen kan fornys efter proceduren i litra punkt 12.4.

12.7. Generalsekretæren inddrager godkendelsen, hvis vedkommende finder, at der er grund til sådan inddragelse. Inddrages godkendelsen, underrettes den pågældende af Europa-Parlamentets tjenestemænd eller øvrige ansatte, der arbejder for en berørt politisk gruppe, der kan anmode om at måtte fremsætte sine bemærkninger over for formanden, inden inddragelsen får virkning, samt de nationale myndigheder.

12.8. Sikkerhedsundersøgelsen foretages med medvirken fra den berørte af Europa-Parlamentets tjenestemænd eller øvrige af Parlamentets ansatte, der arbejder for berørte politiske grupper, og efter anmodning fra generalsekretæren. Den for sikkerhedsundersøgelsen kompetente nationale myndighed er myndigheden i den medlemsstat, hvor den berørte person er statsborger. Hvis der er hjemmel herfor i nationale love og bestemmelser, kan de kompetente nationale sikkerhedsmyndigheder gennemføre undersøgelser af ikke-statsborgere, der skal have adgang til informationer, som er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET.

12.9. Den pågældende af Europa-Parlamentets tjenestemænd eller øvrige af Parlamentets ansatte, der arbejder for de politiske grupper, skal som led i sikkerhedsundersøgelsen udfylde et skema med angivelse af personlige oplysninger.

12.10. Generalsekretæren giver i sin anmodning til den kompetente nationale myndighed nærmere oplysninger om klassifikationsgraden for de oplysninger, som den pågældende tjenestemand i Europa-Parlamentet eller øvrige af Parlamentets ansatte, der arbejder for en berørt politisk gruppe, vil få kendskab til, så den kan foretage sikkerhedsundersøgelsen og afgive udtalelse om, hvilket niveau den pågældende bør godkendes til.

12.11. De bestemmelser om sikkerhedsundersøgelse, som er gældende i vedkommende medlemsstat, herunder bestemmelser om eventuel klageadgang, finder anvendelse i forbindelse med hele den af den kompetente nationale myndighed foretagne sikkerhedsundersøgelses forløb og dens resultater.

12.12. Afgiver den kompetente nationale myndighed positiv udtalelse, kan generalsekretæren godkende den pågældende tjenestemand i Europa-Parlamentet eller øvrige af Parlamentets ansatte, der arbejder for berørte politiske grupper.

12.13. Afgiver den nationale myndighed negativ udtalelse, underrettes den pågældende af Europa-Parlamentets tjenestemænd eller Parlamentets øvrige ansatte, der arbejder for de politiske grupper, og den pågældende kan anmode om at måtte fremsætte sine bemærkninger over for generalsekretæren. Finder Generalsekretæren det nødvendigt, kan vedkommende rette henvendelse til den nationale myndighed og bede om eventuelle yderligere oplysninger. Bekræftes den negative udtalelse, kan der ikke meddeles godkendelse.

12.14. Enhver af Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for de politiske grupper, der godkendes efter punkt 12.4 og 12.5, får i forbindelse med godkendelsen og siden med jævne mellemrum de nødvendige instrukser om beskyttelse af klassificerede oplysninger og om, hvordan de skal beskyttes. Sådanne tjenestemænd og øvrige ansatte underskriver en erklæring som bekræftelse på at have modtaget instrukserne og giver tilsagn om at overholde dem.

12.15. Generalsekretæren kan undtagelsesvis meddele midlertidig godkendelse af en af Europa-Parlamentets tjenestemænd eller Parlamentets øvrige ansatte, der arbejder for de politiske grupper, for et tidsrum på højst seks måneder, mens resultatet af sikkerhedsundersøgelsen som omhandlet punkt 12.11 afventes, forudsat at den kompetente nationale myndighed på forhånd er blevet underrettet, og der ikke er modtaget bemærkninger herfra inden for en måned. Sådanne midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret på niveau TRÈS SECRET UE/EU TOP SECRET eller tilsvarende.

BILAG II

INDLEDNING

Dette bilag indeholder de sikkerhedsmeddelelser, der danner grundlag for en sikker behandling og forvaltning af fortrolige oplysninger i Europa-Parlamentet. Disse sikkerhedsmeddelelser udgør sammen med behandlingsinstrukserne Europa-Parlamentets system til forvaltning af informationssikkerheden, jf. artikel 3, stk. 2, i denne afgørelse.

SIKKERHEDSMEDDELELSE 1

Den sikkerhedsmæssige organisation i Europa-Parlamentet med henblik på beskyttelse af fortrolige oplysninger

SIKKERHEDSMEDDELELSE 2

Forvaltning af fortrolige oplysninger

SIKKERHEDSMEDDELELSE 3

Behandling af fortrolige oplysninger ved hjælp af automatiske kommunikations- og informationssystemer (CIS)

SIKKERHEDSMEDDELELSE 4

Fysisk sikkerhed

SIKKERHEDSMEDDELELSE 5

Industriel sikkerhed

SIKKERHEDSMEDDELELSE 6

Brud på sikkerheden, tab eller kompromittering af fortrolige oplysninger

SIKKERHEDSMEDDELELSE 1

DEN SIKKERHEDSMÆSSIGE ORGANISATION I EUROPA-PARLAMENTET MED HENBLIK PÅ BESKYTTELSE AF FORTROLIGE OPLYSNINGER

1. Generalsekretæren har det overordnede ansvar for en konsekvent anvendelse af denne afgørelse.

Generalsekretæren træffer alle fornødne foranstaltninger til at sikre, at denne afgørelse anvendes i forbindelse med behandling eller opbevaring af fortrolige oplysninger af Europa-Parlamentets medlemmer, tjenestemænd og øvrige ansatte, der arbejder for de politiske grupper, samt af kontrahenter.

2. Generalsekretæren er sikkerhedsmyndighed (SA). Generalsekretæren er i denne egenskab ansvarlig for:

2.1. samordning af alle spørgsmål om beskyttelse af fortrolige oplysninger i forbindelse med Parlamentets virksomhed

2.2. godkendelse af indretningen af et sikret område, sikre læseværelser og sikkert udstyr

2.3. afgørelser om bemyndigelse til videregivelse af klassificerede oplysninger fra Parlamentet til tredjemand i overensstemmelse med artikel 6 i denne afgørelse

2.4. gennemførelse eller iværksættelse af undersøgelser af ethvert tilfælde, hvor der er mistanke om lækage af fortrolige oplysninger i Parlamentet, i samarbejde med Europa-Parlamentets formand, såfremt et medlem af Europa-Parlamentet er involveret i sagen

2.5. opretholdelse af tæt kontakt med sikkerhedsmyndighederne i andre EU-institutioner og -organer og med medlemsstaternes nationale sikkerhedsmyndigheder med henblik på at sikre en optimal samordning af sikkerhedspolitikken for så vidt angår klassificerede oplysninger

2.6. løbende revision af Parlamentets sikkerhedspolitik og sikkerhedsprocedurer samt udstedelse af passende henstillinger på baggrund heraf

2.7. underretning af den nationale sikkerhedsmyndighed (NSA), der har udført en sikkerhedsundersøgelse i henhold til bilag I, del 2, punkt 11.3, om enhver negativ oplysning, der kan berøre denne myndighed.

3. Såfremt medlemmer af Europa-Parlamentet er involveret, varetager generalsekretæren sine ansvarsopgaver i tæt samarbejde med Europa-Parlamentets formand.

4. Generalsekretæren bistås med varetagelsen af sine ansvarsopgaver i punkt 2 og 3 af vicegeneralsekretæren, Direktoratet for Sikkerhed og Risikovurdering, Direktoratet for Informationsteknologi (DIT) og Enheden for Klassificerede Oplysninger (CIU).

4.1. Direktoratet for Sikkerhed og Risikovurdering er ansvarligt for personlige beskyttelsesforanstaltninger og især for sikkerhedsgodkendelsesproceduren, jf. bilag I, del 2. Direktoratet for Sikkerhed og Risikovurdering har også til opgave at:

a) fungere som kontaktpunkt for sikkerhedsmyndighederne i andre EU-institutioner og for NSA'er i spørgsmål vedrørende sikkerhedsgodkendelsesprocedurer for Europa-Parlamentets medlemmer, tjenestemænd og øvrige ansatte, der arbejder for Parlamentets politiske grupper

b) sørge for den nødvendige sikkerhedsinformation vedrørende forpligtelsen til at beskytte klassificerede oplysninger og følgerne af at undlade dette

c) overvåge driften af det sikrede område og de sikre læseværelser inden for Parlamentets område, om nødvendigt i samarbejde med sikkerhedstjenesterne i andre EU-institutioner og med NSA'er

d) gennemgå procedurerne for forvaltning og opbevaring af klassificerede oplysninger, det sikrede område og de sikre læseværelser inden for Parlamentets område, hvor der behandles klassificerede oplysninger, i samarbejde med sikkerhedstjenesterne i andre EU-institutioner og med NSA'er

e) foreslå generalsekretæren passende behandlingsinstrukser.

4.2. DIT er ansvarligt for it-sikkerhedssystemerne til behandling af fortrolige oplysninger i Europa-Parlamentet.

4.3. CIU er ansvarlig for:

a) identifikation af sikkerhedsbehovene med henblik på effektiv beskyttelse af fortrolige oplysninger i samarbejde med Direktoratet for Sikkerhed og Risikovurdering og DIT og med de andre EU-institutioners sikkerhedstjenester

b) identifikation af alle aspekter af forvaltningen og opbevaringen af fortrolige oplysninger inden for Parlamentet som fastlagt i behandlingsinstrukserne

c) driften af det sikrede område

d) forvaltning eller konsultation af fortrolige oplysninger i det sikrede område eller i CIU's sikre læseværelse, jf. artikel 7, stk. 2 og 3, i denne afgørelse

e) forvaltning af CIU-registret

f) underretning af SA om ethvert tilfælde, hvor der er bevis for eller mistanke om brud på sikkerheden, tab eller kompromittering af fortrolige oplysninger, der er overdraget til CIU og opbevares i det sikrede område eller i CIU's sikre læseværelse.

5. Generalsekretæren udnævner endvidere i sin egenskab af SA følgende myndigheder:

a) en sikkerhedsakkrediteringsmyndighed (SAA)

b) en operativ informationssikringsmyndighed (IAOA)

c) en kryptodistributionsmyndighed (CDA)

d) en Tempestmyndighed (TA)

e) en informationssikringsmyndighed (IAA)

Udøvelsen af disse funktioner forudsætter ikke enkelte organisatoriske enheder. De skal have separate mandater. Disse funktioner og det medfølgende ansvar kan imidlertid kombineres eller integreres inden for samme organisatoriske enhed eller opdeles i forskellige organisatoriske enheder, forudsat at interne interessekonflikter og overlapninger mellem arbejdsopgaver undgås.

6. SAA'en skal rådgive om alle sikkerhedsspørgsmål i relation til akkrediteringen af hvert enkelt it-system og -net i Parlamentet ved at:

6.1. sikre, at et CIS overholder de relevante sikkerhedspolitikker og tekniske sikkerhedsretningslinjer, give en udredning om godkendelse af CIS'er til håndtering af klassificerede oplysninger inden for en bestemt klassifikationsgrad i driftsmiljøet og fastlægge betingelserne for akkreditering og kriterierne for fornyet godkendelse

6.2. etablere en sikkerhedsakkrediteringsproces i overensstemmelse med de relevante politikker, der klart angiver de godkendelsesbetingelser, der gælder for et CIS under dens ansvar

6.3. definere en sikkerhedsakkrediteringsstrategi, der fastsætter en detaljeringsgrad for akkrediteringsprocessen svarende til det krævede sikringsniveau

6.4. gennemgå og godkende sikkerhedsrelateret dokumentation, herunder udredninger om risikostyring og residualrisiko, dokumentation for kontrol af sikkerhedsimplementering og procedurerne for sikker drift, og sikre, at dokumentationen er i overensstemmelse med Parlamentets sikkerhedsregler og sikkerhedspolitik

6.5. kontrollere implementeringen af sikkerhedsforanstaltningerne i forbindelse med CIS'et ved at foretage eller få foretaget sikkerhedsvurderinger, -inspektioner eller -revisioner

6.6. fastlægge sikkerhedskrav (f.eks. niveauer for personalesikkerhedsgodkendelse) for stillinger, der er følsomme i CIS-sammenhæng

6.7. godkende eller, hvor det er relevant, deltage i den fælles godkendelse af sammenkoblingen af et CIS med andre CIS'er

6.8. godkende sikkerhedsstandarderne ved teknisk udstyr beregnet til sikker behandling og beskyttelse af klassificerede oplysninger

6.9. sikre, at kryptoprodukter, der benyttes i Parlamentet, er opført på listen over EU-godkendte produkter, samt

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

7. IAOA er ansvarlig for:

7.1. udvikling af sikkerhedsdokumentation i overensstemmelse med sikkerhedspolitikkerne og sikkerhedsretningslinjerne, navnlig udredningen om residualrisikoen, procedurerne for sikker drift og kryptoplanen inden for CIS-akkrediteringsprocessen

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

7.3. overvågning af gennemførelsen og anvendelsen af procedurerne for sikker drift og, hvor det er relevant, uddelegering af operationelt sikkerhedsansvar til systemejeren, som er CIU

7.4. forvaltning og håndtering af kryptoprodukter, sikker opbevaring af kryptomateriale og kontrolleret materiale og om nødvendigt generering af kryptovariabler

7.5. gennemførelse af sikkerhedsanalyserevisioner og -afprøvninger, især for at udarbejde relevante risikorapporter, som krævet af SAA'en

7.6. levering af CIS-specifik uddannelse i informationssikring

7.7. implementering og anvendelse af CIS-specifikke sikkerhedsforanstaltninger.

8. CDA er ansvarlig for:

8.1. at forvalte og stå til regnskab for EU-kryptomateriale

8.2. i tæt samarbejde med SAA'en at sikre, at de relevante procedurer håndhæves, og at der foreligger planer for bogføring, sikker behandling, opbevaring og distribution af alt EU-kryptomateriale, samt

8.3. at sikre overdragelsen af EU-kryptomateriale til eller fra enkeltpersoner eller tjenester, der bruger det.

9. TA er ansvarlig for at sikre, at CIS'er er i overensstemmelse med Tempestpolitikkerne og behandlingsinstrukserne. Den godkender Tempestmodforanstaltninger vedrørende anlæg og produkter til beskyttelse af klassificerede oplysninger inden for en bestemt klassifikationsgrad i driftsmiljøet.

10. IAA er ansvarlig for alle aspekter af forvaltningen og behandlingen af fortrolige oplysninger i Parlamentet og navnlig for:

10.1 udvikling af informationssikkerhed og tekniske sikkerhedsretningslinjer og overvågning af deres effektivitet og relevans

10.2. beskyttelse og forvaltning af tekniske informationer om kryptoprodukter

10.3. sikring af, at de informationssikkerhedsforanstaltninger, der vælges til sikkerhedsbeskyttelse af klassificerede oplysninger, opfylder egnetheds- og udvælgelseskriterierne i de relevante politikker

10.4. sikring af, at kryptoprodukter udvælges i overensstemmelse med egnetheds- og udvælgelseskriterierne i de relevante politikker

10.5. konsultation af systemleverandøren, sikkerhedsaktørerne og brugerrepræsentanterne med hensyn til informationssikkerhed

SIKKERHEDSMEDDELELSE 2

FORVALTNING AF FORTROLIGE OPLYSNINGER

A. **INDLEDNING**

1. Denne sikkerhedsmeddelelse indeholder bestemmelserne om Parlamentets forvaltning af fortrolige oplysninger.

2. Når der udarbejdes fortrolige oplysninger, skal udstederen vurdere fortrolighedsgraden og træffe beslutning om klassificeringen eller påtegningen af disse oplysninger på grundlag af principperne i denne sikkerhedsmeddelelse.

B. **EUCI-KLASSIFIKATION**

3. En beslutning om at klassificere et dokument skal træffes før dets oprettelse. I den forbindelse indebærer klassificering af oplysninger som EUCI, at udstederen på grundlag af en forudgående vurdering af deres fortrolighedsgrad beslutter, at uberettiget videregivelse heraf til en vis grad vil kunne skade Den Europæiske Unions eller en eller flere af dens medlemsstaters eller enkeltpersoners interesser.

4. Når beslutningen om at klassificere oplysningerne er truffet, skal der foretages endnu en forudgående vurdering med henblik på at fastslå den korrekte klassifikationsgrad. Et dokuments klassifikation skal bestemmes af, hvor følsomt dets indhold er.

5. Ansvaret for klassificeringen af oplysninger påhviler alene deres udsteder. Parlamentets tjenestemænd klassificerer oplysninger efter instruks fra generalsekretæren eller med dennes bemyndigelse.

6. Klassificering skal anvendes korrekt og med måde. Udstederen af et dokument, som skal klassificeres, skal undgå enhver tendens til at overklassificere eller underklassificere.

7. Oplysningernes klassifikation er bestemmende for den beskyttelse, de tildeles for så vidt angår personelsikkerhed, fysisk sikkerhed, proceduresikkerhed og informationssikring.

8. Oplysninger, der er berettigede til klassificering, skal påtegnes og behandles i overensstemmelse hermed uanset deres fysiske form. Modtagerne af oplysningerne skal have klar besked om disses klassifikation, enten ved en sikkerhedsklassifikationspåtegning (hvis de afgives skriftligt, det være sig på papir eller i CIS) eller ved en meddelelse (hvis oplysningerne afgives mundtligt, f.eks. under en samtale eller et lukket møde). Klassificeret materiale skal forsynes med en fysisk påtegning, således at dets sikkerhedsklassifikation let kan fastslås.

9. EUCI i elektronisk form må kun udarbejdes inden for et akkrediteret CIS. Selve de klassificerede oplysninger samt deres filnavn og lagringsmedie (hvis der er tale om et eksternt medie såsom en CD-ROM eller en USB-nøgle) skal være forsynet med den relevante sikkerhedsklassifikationspåtegning.

10. Oplysninger skal klassificeres, så snart de tager form. For eksempel skal personlige noter, tekstudkast og e-mailbeskeder indeholdende oplysninger, der berettiger til klassificering, mærkes som EUCI lige fra begyndelsen samt udarbejdes og behandles i overensstemmelse med denne afgørelse og dens behandlingsinstrukser i såvel fysisk som teknisk henseende. Sådanne oplysninger kan så efterhånden udvikle sig til et officielt dokument, som for sin del vil blive korrekt mærket og behandlet. Det kan i løbet af udarbejdelsesprocessen blive nødvendigt at revurdere et officielt dokument og tildele det en højere eller lavere klassifikation.

11. Udstederen kan beslutte at tildele en standardklassifikation til kategorier af oplysninger, den pågældende frembringer med jævne mellemrum. Udstederen skal dog i den forbindelse sikre sig, at den pågældende ikke systematisk over- eller underklassificerer specifikke oplysninger.

12. EUCI skal altid være forsynet med en sikkerhedsklassifikationspåtegning, der svarer til deres klassifikationsgrad.

B.1. ***Klassifikationsgrader***

13. EUCI klassificeres i en af følgende grader:

— »TRÈS SECRET UE/EU TOP SECRET«, som defineret i artikel 2, litra d) i denne afgørelse, dvs. oplysninger, som, hvis de kompromitteres, kan forventes at:

a) medføre en direkte trussel mod den indre stabilitet af Unionen eller en eller flere medlemsstater, tredjelande eller internationale organisationer

b) forvolde særlig alvorlig skade på forbindelserne med tredjelande eller internationale organisationer

c) føre direkte til omfattende tab af menneskeliv

d) forvolde overordentlig stor skade på den driftsmæssige effektivitet eller sikkerhed for medlemsstaternes eller andre bidragyderes udsendte personel eller for den fortsatte effektivitet af særligt værdifulde sikkerheds- eller efterretningsoperationer

e) forvolde alvorlig langsigtet skade på Unionens eller medlemsstaternes økonomi

— »SECRET UE/EU SECRET«, som defineret i artikel 2, litra d) i denne afgørelse, dvs. oplysninger, som, hvis de kompromitteres, kan forventes at:

a) skabe betydelige internationale spændinger

b) forvolde alvorlig skade på forbindelserne med tredjelande og internationale organisationer

c) være direkte livstruende eller være til alvorlig skade for den offentlige orden eller enkeltpersoners sikkerhed eller frihed

d) forvolde skade på vigtige handelsmæssige eller politiske forhandlinger og derved skabe væsentlige operationelle problemer for Unionen eller medlemsstaterne

e) forvolde alvorlig skade på medlemsstaternes operationelle sikkerhed eller på effektiviteten af meget værdifulde sikkerheds- eller efterretningsaktiviteter

f) forvolde betydelig materiel skade på Unionens eller medlemsstaternes finansielle, monetære, økonomiske og handelsmæssige interesser

g) undergrave den finansielle levedygtighed af større organisationer eller aktører i væsentlig grad, eller

h) skabe alvorlige hindringer for udviklingen eller gennemførelsen af EU-politikker med store økonomiske, handelsmæssige eller økonomiske konsekvenser

— »CONFIDENTIEL UE/EU CONFIDENTIEL«, som defineret i artikel 2, litra d) i denne afgørelse, dvs. oplysninger, som, hvis de kompromitteres, kan forventes at:

a) forvolde alvorlig skade på diplomatiske forbindelser, f.eks. ved at afføde formelle protester eller andre sanktioner

b) bringe enkeltpersoners sikkerhed eller frihed i fare

c) bringe resultatet af handelsmæssige eller politiske forhandlinger i alvorlig fare og derved skabe operationelle problemer for Unionen eller dens medlemsstater

d) forvolde skade på medlemsstaternes operationelle sikkerhed eller på effektiviteten af værdifulde sikkerheds- eller efterretningsaktiviteter

e) undergrave den finansielle levedygtighed af større organisationer eller aktører i væsentlig grad

f) hindre efterforskningen af eller gøre det lettere at begå kriminalitet eller terrorvirksomhed

g) modarbejde Unionens eller medlemsstaternes finansielle, monetære, økonomiske og handelsmæssige interesser i væsentlig grad

h) skabe alvorlige hindringer for udviklingen eller gennemførelsen af EU-politikker med store økonomiske, handelsmæssige eller økonomiske konsekvenser

— »RESTREINT UE/EU RESTRICTED«, som defineret i artikel 2, litra d) i denne afgørelse, dvs. oplysninger, som, hvis de kompromitteres, kan forventes at:

a) være til skade for Unionens generelle interesser

b) være til skade for diplomatiske forbindelser

c) skabe alvorlige problemer for enkeltpersoner eller virksomheder

d) være til ugunst for Unionen eller medlemsstaterne i handelsmæssige eller politiske forhandlinger

e) gøre det vanskeligere at opretholde en effektiv sikkerhed inden for Unionen eller medlemsstaterne

f) hindre en effektiv udvikling eller gennemførelse af Unionens politikker

g) undergrave den korrekte forvaltning af Unionen og dens aktiviteter

h) medføre brud på tilsagn afgivet af Parlamentet om opretholdelse af klassifikationsstatus for oplysninger fra tredjemand

i) medføre overtrædelse af lovgivningsmæssige begrænsninger for videregivelse af oplysninger

j) forårsage økonomiske tab eller gøre det lettere at opnå en uberettiget gevinst eller fordel for enkeltpersoner eller virksomheder, eller

k) skade efterforskningen af eller gøre det lettere at begå kriminalitet

B.2. ***Klassificering af aktsamlinger, følgeskrivelser og tekstdele***

14. En følgeskrivelse skal klassificeres på niveau med det bilag, der har den højeste klassifikationsgrad. Udstederen skal klart angive, på hvilket niveau følgeskrivelsen skal klassificeres, hvis den adskilles fra bilagene. I tilfælde af, at følgeskrivelsen ikke behøver ikke at blive klassificeret, skal den forsynes med en påtegning om, at den skal afklassificeres, hvis den adskilles fra sine bilag.

15. Dokumenter eller aktsamlinger, der indeholder dele med forskellig klassifikationsgrad, skal i videst muligt omfang struktureres på en sådan måde, at dele med en afvigende klassifikationsgrad let kan identificeres og udskilles, hvis det er nødvendigt. Et dokuments eller en aktsamlings overordnede klassifikationsgrad må ikke være lavere end den del, der har den højeste klassifikationsgrad.

16 Et dokuments enkelte sider, afsnit og dele samt bilag, tillæg og vedhæftelser kan kræve forskellige klassifikationsgrader og skal klassificeres i overensstemmelse hermed. Der kan i dokumenter, som indeholder EUCI, anvendes standardforkortelser til at angive klassifikationsgraden af tekstdele af mindre end en sides længde.

17. Når oplysninger er indsamlet fra forskellige kilder, skal det endelige produkt gennemgås for at fastlægge dets samlede klassifikationsgrad, da det kan kræve en højere klassifikationsgrad end dets enkelte bestanddele.

C. **ANDRE FORTROLIGE OPLYSNINGER**

18. »Andre fortrolige oplysninger« skal mærkes i overensstemmelse med punkt E i denne sikkerhedsmeddelelse og i behandlingsinstrukserne.

D. **UDARBEJDELSE AF FORTROLIGE OPLYSNINGER**

19. Fortrolige oplysninger må kun udarbejdes af personer, som er bemyndigede hertil i kraft af denne afgørelse eller en bemyndigelse fra SA.

20. Fortrolige oplysninger må ikke indlæses i internet- eller intranetdokumentforvaltningssystemer.

D.1. ***Udarbejdelse af EUCI***

21. EUCI klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET må kun udarbejdes af personer, som er bemyndigede hertil i kraft af denne afgørelse eller allerede er i besiddelse af en bemyndigelse i henhold til artikel 4, stk. 1, i denne afgørelse.

22. EUCI klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET må kun udarbejdes inden for det sikrede område.

23. Følgende regler gælder for udarbejdelse af EUCI:

a) hver side skal være tydeligt mærket med klassifikationsgraden

b) hver side skal være nummereret og angive det samlede sideantal

c) dokumentet skal være forsynet med et referencenummer og en angivelse af sit emne, som ikke i sig selv må udgøre en klassificeret oplysning, medmindre dette er anført

d) dokumentet skal være forsynet med en dato på første side

e) første side af ethvert dokument klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET skal indeholde en liste over alle bilag

f) dokumenter klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET skal på hver side være forsynet med et eksemplarnummer, hvis de skal udsendes i flere eksemplarer. Hvert eksemplar skal endvidere på første side være forsynet med en angivelse af det samlede antal eksemplarer og sider, og

g) hvis dokumentet indeholder henvisninger til andre dokumenter med klassificerede oplysninger, der er modtaget fra andre EU-institutioner, eller hvis det indeholder klassificerede oplysninger hidrørende fra disse dokumenter, skal det have samme klassificeringsgrad som disse dokumenter og må ikke uden forudgående skriftligt samtykke fra udstederen udleveres til andre personer end dem, der er nævnt i distributionslisten for det eller de oprindelige dokumenter med klassificerede oplysninger.

24. Udstederen skal bevare kontrollen med de EUCI, som den pågældende har udarbejdet. Der skal indhentes skriftligt samtykke fra udstederen, inden en EUCI kan:

a) ned- eller afklassificeres

b) benyttes til andre formål end dem, udstederen har fastlagt

c) videregives til en tredjestat eller international organisation

d) videregives til andre personer, institutioner, lande eller internationale organisationer end de modtagere, som udstederen oprindeligt gav adgang til den pågældende oplysning

e) videregives til en kontrahent eller potential kontrahent i en tredjestat

f) kopieres eller oversættes, såfremt oplysningen er klassificeret på niveau TRES SECRET UE/EU TOP SECRET

g) destrueres.

D.2. ***Udarbejdelse af andre fortrolige oplysninger***

25. Generalsekretæren kan i sin egenskab af SA træffe afgørelse om, hvorvidt en bestemt funktion, tjeneste og/eller enkeltperson skal have bemyndigelse til at udarbejde »andre fortrolige oplysninger«.

26. »Andre fortrolige oplysninger« skal være forsynet med en af de påtegninger, som er fastlagt i behandlingsinstrukserne.

27. Følgende regler gælder for udarbejdelse af »andre fortrolige oplysninger«:

a) påtegningen skal være anført øverst på dokumentets første side

b) hver side skal være nummereret og angive det samlede sideantal

c) dokumentet skal være forsynet med et referencenummer og en angivelse af sit emne

d) dokumentet skal være forsynet med en dato på første side

e) dokumentets sidste side skal indeholde en liste over alle bilag.

28. Udarbejdelsen af »andre fortrolige oplysninger« er underlagt specifikke regler og procedurer, som er fastlagt i behandlingsinstrukserne.

E. **SIKKERHEDSANGIVELSER OG PÅTEGNINGER**

29. Formålet med sikkerhedsangivelser og påtegninger er at kontrollere informationsstrømmen og begrænse adgangen til fortrolige oplysninger på grundlag af »need to know«-princippet.

30. Når der anvendes eller påføres sikkerhedsangivelser og påtegninger, er det vigtigt at undgå forveksling med sikkerhedsklassifikationerne for EUCI: »RESTREINT UE/EU RESTRICTED«, »CONFIDENTIEL UE/EU CONFIDENTIAL«, »SECRET UE/EU SECRET«, »TRES SECRET UE/EU TOP SECRET«.

31. Der skal i behandlingsinstrukserne fastlægges specifikke regler for anvendelsen af sikkerhedsangivelser og påtegninger sammen med en liste over af Europa-Parlamentet godkendte sikkerhedspåtegninger.

E.1. ***Sikkerhedsangivelser***

32. Sikkerhedsangivelser må kun bruges sammen med en sikkerhedsklassifikation og må ikke anvendes særskilt på dokumenter. En sikkerhedsangivelse kan anvendes på EUCI for at:

a) begrænse gyldighedsperioden af en klassifikationsgrad (med automatisk ned- eller afklassificering af klassificerede oplysninger)

b) begrænse distributionen af de pågældende EUCI

c) fastlægge særlige behandlingsordninger i tilgift til dem, der gælder for den pågældende klassifikationsgrad.

33. Den ekstra kontrol, som er forbundet med behandling og opbevaring af dokumenter indeholdende EUCI, indebærer ekstra byrder for alle berørte. For at minimere det arbejde, dette indebærer, er det god praksis, at man i forbindelse med oprettelsen af sådanne dokumenter fastsætter en frist eller en begivenhed, efter hvilken klassificeringen automatisk udløber, og oplysningerne i dokumentet skal ned- eller afklassificeres.

34. Hvis et dokument omhandler et bestemt arbejdsområde, og distributionen heraf skal være begrænset, og/eller hvis det kræver en særlig behandlingsordning, kan en erklæring herom føjes til dets klassifikationsgrad for at gøre det lettere at identificere målgruppen.

E.2. ***Påtegninger***

35. Påtegninger udgør ikke en sikkerhedsklassifikation. De har kun til formål at give konkrete instrukser om behandlingen af dokumentet og må ikke bruges til at beskrive dokumentets indhold.

36. Påtegninger kan anføres særskilt på dokumenter eller bruges sammen med en sikkerhedsklassifikation.

37. Som hovedregel skal påpegninger anvendes på oplysninger, som er omfattet af tavshedspligt (som omhandlet i TEUF artikel 339 og artikel 17 i tjenestemandsvedtægten) eller som Parlamentet skal beskytte af juridiske årsager, men som det ikke er nødvendigt eller muligt at klassificere.

E.3. ***Brug af påtegninger i CIS'er***

38. Reglerne om brugen af påtegninger finder også anvendelse for akkrediterede CIS'er.

39. SAA'en fastlægger specifikke regler om brugen af påtegninger i akkrediterede CIS'er.

F. **MODTAGELSE AF OPLYSNINGER**

40. Inden for Parlamentet er kun CIU berettiget til at modtage oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende fra tredjeparter.

41. Hvad angår oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende kan såvel CIU som det kompetente parlamentariske organ/den kompetente hvervsindehaver være ansvarlig for at modtage dem fra tredjemand og for at anvende de i denne sikkerhedsmeddelelse fastsatte principper.

G. **REGISTRERING**

42. Registrering betyder anvendelsen af procedurer til registrering af fortrolige oplysningers livscyklus, herunder deres udbredelse, konsultation og destruktion.

43. I denne sikkerhedsmeddelelse betyder »journal« et register, hvori der navnlig registreres datoer og klokkeslæt for, hvornår fortrolige oplysninger:

a) tilgår eller forlader det respektive sekretariat for det parlamentariske organ/hvervsindehaveren eller i påkommende tilfælde CIU

b) konsulteres af eller sendes til en sikkerhedsgodkendt person samt

c) destrueres.

44. Udstederen af klassificerede oplysninger er ansvarlig for at påtegne den oprindelige erklæring ved udarbejdelsen af et dokument, der indeholder denne type oplysninger. Denne erklæring skal meddeles CIU, når dokumentet oprettes.

45. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIEL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET eller tilsvarende må kun registreres af CIU af sikkerhedshensyn. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og andre fortrolige oplysninger, modtaget fra tredjeparter, registreres til administrative formål af de tjenestegrene, der er ansvarlige for den officielle modtagelse af dokumentet, hvad enten det er CIU eller sekretariatet for det parlamentariske organ/hvervsindehaveren. »Andre fortrolige oplysninger«, der udarbejdes inden for Parlamentet, registreres til administrative formål af udstederen.

46. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIEL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET eller tilsvarende registreres særligt, når:

a) de udarbejdes

b) når de tilgår eller forlader CIU, samt

c) når de tilgår eller forlader CIS'et.

47. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende registreres særligt, når:

a) de udarbejdes

b) de tilgår eller forlader det respektive sekretariat for det parlamentariske organ/hvervsindehaveren eller CIU, samt

c) når de tilgår eller forlader CIS'et.

48. Registrering af fortrolige oplysninger kan udføres på papir eller i elektroniske journaler/i et CIS.

49. For oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende eller som »andre fortrolige oplysninger« registreres som minimum følgende:

a) dato og tidspunkt for, hvornår de tilgår eller forlader det respektive sekretariat for det parlamentariske organ/hvervsindehaveren eller i påkommende tilfælde CIU

b) dokumenttitel, klassifikationsgrad eller påtegning, klassifikationens/påtegningens udløbsdato og alle referencenumre, som dokumentet har fået tildelt.

50. For oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende registreres som minimum følgende:

a) dato og tidspunkt for, hvornår de tilgår eller forlader CIU

b) dokumenttitel, klassifikationsgrad eller påtegning, eventuelle referencenumre, som dokumentet har fået tildelt, og klassifikationens/påtegningens udløbsdato

c) nærmere oplysninger om udstederen

d) et register over identiteten af enhver person, der har fået tildelt adgang til dokumentet, og datoen, hvor der er givet adgang til dokumentet

e) et register over kopier eller oversættelser af dokumentet

f) datoen og tidspunktet for, hvornår kopier eller oversættelser af dokumentet forlader eller returneres til CIU, og nærmere oplysninger om, hvor de er blevet sendt hen, og hvem der har returneret dem

g) dato og tidspunkt for, hvornår dokumentet er destrueret og af hvem i overensstemmelse med Parlamentets sikkerhedsregler om destruktion, samt

h) dokumentets af- eller nedklassificering.

51. Journaler klassificeres eller mærkes om nødvendigt. Journaler for oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende registreres med samme klassifikationsgrad.

52. Klassificerede oplysninger kan registreres:

a) i en samlet journal eller

b) i separate journaler efter klassifikationsgrad, efter deres status som ind- eller udgående og efter oprindelses- eller bestemmelsessted.

53. I forbindelse med elektronisk behandling i et CIS kan registreringsprocedurerne gennemføres ved processer i selve CIS'et, hvis de opfylder krav svarende til kravene angivet ovenfor. Når EUCI forlader CIS'ets perimeter, gælder ovenstående registreringsprocedure.

54. CIU opbevarer en fortegnelse over alle klassificerede oplysninger, der udsendes af Parlamentet til tredjepart, og klassificerede oplysninger, der modtages af Parlamentet fra tredjepart.

55. Når registreringen af oplysninger klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende er gennemført, kontroller CIU, om modtageren har en gyldig sikkerhedsgodkendelse. Hvis dette er tilfældet, underrettes modtageren af CIU. Konsultation af klassificerede oplysninger må først finde sted, når dokumentet, der indeholder disse, er blevet registreret.

H. **FORDELING**

56. Udstederen skal udarbejde den første distributionsliste for de EUCI, som den pågældende har udarbejdet.

57. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED og »andre fortrolige oplysninger« udarbejdet af Parlamentet skal distribueres inden for Parlamentet af udstederen i overensstemmelse med de relevante behandlingsinstrukser og på grundlag af need to know-princippet. For så vidt angår oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, der er udarbejdet af Parlamentet inden for det sikrede område, skal distributionslisten (og alle øvrige instrukser vedrørende distribution) gives til CIU, som er ansvarlig for forvaltningen heraf.

58. EUCI udarbejdet af Parlamentet kan kun distribueres til tredjeparter af CIU på grundlag af need to know-princippet.

59. Fortrolige oplysninger, der enten modtages af CIU eller af et parlamentarisk organ eller en hvervsindehaver, som indgav anmodningen herom, skal distribueres i overensstemmelse med udstederens instrukser.

I. **BEHANDLING, OPBEVARING OG KONSULTATION**

60. Behandling, opbevaring og konsultation af fortrolige oplysninger skal ske i overensstemmelse med sikkerhedsmeddelelse 4 og behandlingsinstrukserne.

J. **KOPIERING/OVERSÆTTELSE/TOLKNING AF KLASSIFICEREDE OPLYSNINGER**

61. Dokumenter indeholdende oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende må kun kopieres eller oversættes efter udstederens forudgående skriftlige samtykke. Dokumenter indeholdende oplysninger klassificeret på niveau SECRET UE/EU SECRET eller tilsvarende eller på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende må kopieres eller oversættes efter instruks fra den person, der er i besiddelse af den, forudsat at udstederen ikke har forbudt dette.

62. Hver kopi af et dokument indeholdende oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET EU eller CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende skal registreres af sikkerhedsmæssige årsager.

63. De sikkerhedsforanstaltninger, der gælder for det oprindelige dokument, som indeholder de klassificerede oplysninger, gælder også for kopier og oversættelser af samme.

64. Dokumenter, der modtages fra Rådet, bør modtages på alle officielle sprog.

65. Kopier og/eller oversættelser af dokumenter indeholdende klassificerede oplysninger kan rekvireres af udstederen eller af den person, der er i besiddelse af kopien. Kopier af dokumenter indeholdende oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, og derover eller tilsvarende må kun kopieres inden for det sikrede område og kun på kopimaskiner, som indgår i et akkrediteret CIS. Kopier af dokumenter indeholdende oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt andre fortrolige oplysninger skal foretages på godkendt reproduktionsudstyr, som befinder sig på Parlamentets område.

66. Alle kopier og oversættelser af et dokument eller dele af kopier af dokumenter indeholdende fortrolige oplysninger skal mærkes, nummereres og registreres på passende vis.

67. Der må ikke laves flere kopier end absolut nødvendigt. Alle kopier skal destrueres i overensstemmelse med behandlingsinstrukserne efter konsultationen.

68. Kun tolke og oversættere, der er tjenestemænd i Parlamentet, kan få adgang til klassificerede dokumenter.

69. Tolke og oversættere med adgang til dokumenter indeholdende oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende skal have den nødvendige sikkerhedsgodkendelse.

70. Tolke eller oversættere, der arbejder med dokumenter indeholdende oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, skal arbejde inden for det sikrede område.

K. **NEDKLASSIFICERING, AFKLASSIFICERING OG FJERNELSE AF MÆRKNING AF FORTROLIGE OPLYSNINGER**

K.1. ***Generelle principper***

71. Fortrolige oplysninger skal afklassificeres, nedklassificeres eller have mærkningen fjernet, når det ikke længere er nødvendigt at beskytte oplysningerne, eller når det ikke længere er nødvendigt at bevare den oprindelige klassifikationsgrad.

72. Det kan ligeledes være nødvendigt at træffe beslutning om at nedklassificere, afklassificere eller fjerne mærkningen fra oplysninger, der er indeholdt i dokumenter udarbejdet i Parlamentet, på ad hoc-basis, f.eks. ved besvarelsen af en begæring om aktindsigt fremsat af offentligheden eller en anden EU-institution, eller på initiativ af CIU eller et parlamentarisk organ/en hvervsindehaver.

73. På det tidspunkt, hvor EUCI udarbejdes, angiver udstederen så vidt muligt, om de pågældende EUCI kan nedklassificeres eller afklassificeres på en bestemt dato eller efter en bestemt begivenhed. Hvis det ikke er muligt at lave en sådan angivelse, tager CIU eller det parlamentariske organ/hvervsindehaveren, der råder over oplysningerne, klassifikationsgraden af EUCI op til revision mindst hver femte år. EUCI må under alle omstændigheder kun nedklassificeres eller afklassificeres med udstederens forudgående skriftlige samtykke.

74. Hvis det ikke kan fastslås eller spores, hvem udstederen af EUCI er for så vidt angår dokumenter udarbejdet i Parlamentet, tager SA, evt. efter høring af CIU, det pågældende EUCI's klassifikationsniveau op til revision på grundlag af et forslag fra det pågældende parlamentariske organ/den hvervsindehaver, som råder over de pågældende oplysninger.

75. CIU eller det parlamentariske organ/den hvervsindehaver, som råder over oplysningerne, er ansvarlig for at underrette modtageren/modtagerne om, at oplysningerne er blevet afklassificeret eller nedklassificeret, og disse modtagere har derpå ansvar for at underrette enhver efterfølgende modtager, til hvem de har sendt eller kopieret dokumentet.

76. Afklassificeringen, nedklassificeringen eller fjernelsen af mærkningen af oplysninger indeholdt i et dokument skal registreres.

K.2. ***Afklassificering***

77. EUCI kan afklassificeres helt eller delvist. EUCI kan afklassificeres delvist, når det ikke længere skønnes nødvendigt at beskytte en bestemt del af det dokument, som indeholder oplysningerne, men fortsat er nødvendigt at beskytte den resterende del.

78. Når revisionen af EUCI indeholdt i et dokument, som er udarbejdet i Parlamentet, resulterer i en beslutning om afklassificering, skal der tages højde for, om dokumentet eventuelt kan offentliggøres, eller om det skal bære en distributionspåtegning (dvs. offentliggøres ikke).

79. Når EUCI afklassificeres, skal afklassificeringen registreres i journalen med angivelse af følgende data: datoen for afklassificeringen, navnet på den person, der anmodede herom og gav bemyndigelse til afklassificeringen, det afklassificerede dokuments referencenummer og dets endelige bestemmelsessted.

80. De gamle klassifikationspåpegninger i det afklassificerede dokument og på alle kopier deraf skal markeres med gennemstregning. Dokumenterne og alle kopier deraf skal opbevares i overensstemmelse hermed.

81. Efter delvis afklassificering af klassificerede oplysninger skal der udarbejdes et afklassificeret uddrag af den afklassificerede del, som skal opbevares på passende vis. Den kompetente tjeneste skal registrere:

a) datoen for den delvise afklassificering

b) navnet på de personer, der anmodede herom og gav bemyndigelse til afklassificeringen, samt

c) det afklassificerede uddrags referencenummer.

K.3. ***Nedklassificering***

82. Efter nedklassificering af klassificerede oplysninger registreres de dokumenter, der indeholder dem, i de journaler, der svarer til både den gamle og den nye klassifikationsgrad. Der skal føres fortegnelse over datoen for nedklassificeringen samt navnet på den person, der bemyndigede den.

83. Dokumentet, som indeholder de nedklassificerede oplysninger, samt alle kopier heraf skal klassificeres med den nye klassifikationsgrad og opbevares på passende måde.

L. **DESTRUKTION AF FORTROLIGE OPLYSNINGER**

84. Fortrolige oplysninger (i papirform eller i elektronisk form), som der ikke længere er brug for, skal destrueres eller slettes i overensstemmelse med behandlingsinstrukserne og de relevante regler for arkivering af dokumenter.

85. Oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende eller som SECRET UE/EU SECRET eller tilsvarende, skal destrueres af CIU. Destruktionen skal ske i overværelse af en person, der er sikkerhedsgodkendt til mindst samme klassifikationsgrad som de oplysninger, der skal destrueres.

86. Oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende kan kun destrueres efter udstederens forudgående skriftlige samtykke.

87. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende skal destrueres og bortskaffes af CIU på instruks fra udstederen eller fra en kompetent myndighed. Journalerne og andre registre ajourføres i overensstemmelse hermed. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende skal destrueres og bortskaffes af enten CIU eller af det relevante parlamentariske organ/hvervsindehaveren.

88. Den tjenestemand, som er ansvarlig for destruktionen, og den relevante person, der overværer destruktionen, skal underskrive en destruktionsattest, der skal opbevares og arkiveres i CIU. CIU skal sammen med distribueringsformularerne opbevare destruktionsattesterne for oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende i mindst ti år, og oplysninger klassificeret på niveau SECRET UE/EU SECRET eller tilsvarende samt oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller tilsvarende i mindst fem år.

89. Dokumenter, der indeholder klassificerede oplysninger, skal destrueres ved hjælp af metoder, som opfylder de relevante EU-standarder eller tilsvarende standarder, for at forhindre hel eller delvis rekonstruktion.

90. Edb-lagringsmedier, der har været anvendt til klassificerede oplysninger, skal destrueres i overensstemmelse med de relevante behandlingsinstrukser.

91. Destruktion af klassificerede oplysninger skal registreres i den relevante journal med angivelse af følgende data:

a) dato og klokkeslæt for destruktionen

b) navnet på den tjenestemand, som er ansvarlig for destruktionen

c) identifikation af de destruerede dokumenter eller kopier

d) de destruerede EUCI-ers originale fysiske form

e) destruktionsmetode, samt

f) destruktionssted.

M. **ARKIVERING**

92. Klassificerede oplysninger, herunder alle følgeskrivelser, bilag, depotudskrifter og/eller andre dele af dossieret skal overføres til det sikre arkiv i det sikrede område seks måneder efter den sidste konsultation og senest et år efter deponeringen. Der skal fastlægges detaljerede regler for arkivering af klassificerede oplysninger i behandlingsinstrukserne.

93. For så vidt angår andre fortrolige oplysninger finder de almindelige regler om dokumenthåndtering anvendelse, uden at dette berører andre specifikke bestemmelser for håndtering af sådanne dokumenter.

SIKKERHEDSMEDDELELSE 3

BEHANDLING AF FORTROLIGE OPLYSNINGER VED HJÆLP AF AUTOMATISKE KOMMMUNIKATIONS- OG INFORMATIONSSYSTEMER (CIS)

A. **INFORMATIONSSIKRING AF KLASSIFICEREDE OPLYSNINGER BEHANDLET I INFORMATIONSSYSTEMER**

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

2. Ved kommmunikations- og informationssystemer (CIS), der behandler klassificerede oplysninger, forstås et system, der gør det muligt at behandle oplysninger i elektronisk form. Et sådant informationssystem skal omfatte alle de aktiver, der er nødvendige for dets drift, herunder infrastrukturer, organisation, personale og informationsressourcer.

3. CIS skal behandle klassificerede oplysninger i overensstemmelse med begrebet IA.

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

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

a) autenticitet: sikkerhed for, at informationer er ægte og kommer fra bona fide-kilder

b) tilgængelighed: det forhold, at informationer er tilgængelige og kan anvendes på anmodning af en autoriseret enhed

c) fortrolighed: det forhold, at informationer ikke videregives til uautoriserede personer, enheder eller processer

d) integritet: sikring af informationernes og aktivernes rigtighed og fuldstændighed

e) uafviselighed: evnen til at bevise, at en handling eller begivenhed har fundet sted, så denne handling eller begivenhed ikke senere kan benægtes.

B. **INFORMATIONSSIKRINGSPRINCIPPER**

6. Nedenstående bestemmelser er grundlaget for sikkerhedsbeskyttelse af al behandling af klassificerede oplysninger i CIS'er. Detaljerede krav til gennemførelse af disse bestemmelser defineres i sikkerhedspolitikker og sikkerhedsretningslinjer for informationssikring.

B.1. ***Sikkerhedsrisikostyring***

7. Sikkerhedsrisikostyringen skal være en integrerende del af at fastlægge, udvikle, drive og opretholde CIS'er. Risikostyringen (vurdering, behandling, accept og kommunikation) skal foregå som en gentagelsesproces, der gennemføres i fællesskab af repræsentanter for systemejere, projektmyndigheder, driftsmyndigheder og sikkerhedsgodkendelsesmyndigheder, som fastlagt i sikkerhedsmeddelelse 1, under anvendelse af en gennemprøvet, gennemsigtig og fuldt forståelig risikovurderingsproces. Anvendelsesområdet for CIS'et og dets aktiver skal klart defineres fra starten af risikostyringsprocessen.

8. De kompetente myndigheder skal, som fastlagt i sikkerhedsmeddelelse 1, tage de potentielle trusler mod CIS'er op til revision og opretholde ajourførte og præcise trusselvurderinger, der afspejler det aktuelle operative miljø. De skal hele tiden ajourføre deres viden om spørgsmål i forbindelse med sårbarhed og regelmæssigt tage sårbarhedsvurderingen op til revision med afsæt i et informationsteknologimiljø (it-miljø) i stadig forandring.

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

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

B.2. ***Sikkerhed i hele CIS'ets livscyklus***

11. Opretholdelse af sikkerheden skal være et krav gennem hele CIS'ets livscyklus fra startfasen, til det tages ud af drift.

12. Rollefordelingen og samspillet mellem de enkelte aktører i et CIS med hensyn til dets sikkerhed skal fastlægges for hver fase af livscyklussen.

13. Et CIS, herunder dets tekniske og ikke-tekniske sikkerhedsforanstaltninger, skal gennemgå sikkerhedstests under akkrediteringsprocessen for at sikre, at det relevante sikkerhedsniveau er nået, og kontrollere, at CIS'et, herunder dets tekniske og ikke-tekniske sikkerhedsforanstaltninger, er korrekt gennemført, integreret og konfigureret.

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

15. Sikkerhedsdokumentationen for et CIS skal udvikles i løbet af dets livscyklus som en integrerende del af processen for håndtering af ændringer.

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

B.3. ***Bedste praksis***

17. IAA'en udvikler bedste praksis for beskyttelse af klassificerede oplysninger, der behandles i et CIS. Retningslinjerne for bedste praksis skal omfatte de tekniske, fysiske, organisatoriske og proceduremæssige sikkerhedsforanstaltninger for CIS'er, som bevisligt er effektive med hensyn til imødegåelse af trusler og sårbarheder.

18. Sikkerhedsbeskyttelsen af klassificerede oplysninger, der behandles i et CIS, skal trække på de erfaringer, som enheder involveret i IA har gjort.

19. Formidlingen og den efterfølgende gennemførelse af bedste praksis skal bidrage til at nå et tilsvarende sikringsniveau for de forskellige CIS'er, der drives af det sekretariat i Parlamentet, der behandler klassificerede oplysninger.

B.4. ***Dybdeforsvar***

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

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

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

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

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

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

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

21. De kompetente myndigheder, jf. sikkerhedsmeddelelse 1, skal sikre, at de kan imødegå hændelser, der kan overskride organisatoriske og nationale grænser, så de kan koordinere svar og udveksle oplysninger om disse hændelser og den hermed forbundne risiko (edb-nødberedskabskapaciteter).

B.5. ***Minimalisme- og »least privilege«-princippet***

22. Der skal for at undgå unødvendige risici kun implementeres de funktioner, det udstyr og de tjenester, der er afgørende for at opfylde operationelle behov.

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

B.6. ***Bevidsthed om informationssikring (IA)***

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

a) det forhold, at sikkerhedssvigt i betydelig grad kan skade CIS'er, der behandler klassificerede oplysninger

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

c) deres individuelle ansvar for CIS'ers sikkerhed alt efter af deres roller inden for systemerne og processerne.

25. For at sikre, at sikkerhedsansvaret forstås, skal IA-uddannelse og -bevidsthedstræning være obligatorisk for alt berørt personale, herunder på ledelsesniveau, medlemmer af Europa-Parlamentet og CIS-brugere.

B.7. ***Evaluering og godkendelse af it-sikkerhedsprodukter***

26. CIS'er, der behandler oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, skal sikkerhedsbeskyttes, således at oplysningerne ikke kan kompromitteres gennem utilsigtede elektromagnetiske emissioner (Tempestsikkerhedsforanstaltninger).

27. Hvis beskyttelsen af klassificerede oplysninger sker ved hjælp af kryptoprodukter, skal sådanne produkter være godkendt af SAA'en som EU-godkendte kryptoprodukter.

28. Ved elektronisk transmission af klassificerede oplysninger skal der anvendes godkendte kryptoprodukter. Uanset dette krav kan der i nødsituationer følges specifikke procedurer eller anvendes specifikke tekniske konfigurationer, jf. punkt 41-44.

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

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

31. SAA skal godkende sikkerhedsretningslinjer for kvalifikation og godkendelse af ikke-kryptografiske it-sikkerhedsprodukter.

B.8. ***Transmission inden for det sikrede område***

32. Ved transmission af klassificerede oplysninger inden for det sikrede område kan ikke-krypteret distribution eller kryptering på et lavere niveau anvendes på grundlag af resultatet af en risikostyringsproces og med forbehold af godkendelse fra SAA'en.

B.9. ***Sikker sammenkobling af CIS'er***

33. Ved systemsammenkobling forstås direkte kobling af to eller flere it-systemer med henblik på udveksling af data og andre informationsressourcer i en eller flere retninger.

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

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

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

b) den pågældende sammenkoblingen skal gennemgå en risikostyrings- og akkrediteringsproces og godkendes af den kompetente SAA

c) der skal oprettes beskyttelsestjenester (PS) rundt om alle CIS'er.

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

37. Hvis det ubeskyttede eller offentlige netværk udelukkende anvendes som bærer, og dataene er krypteret ved hjælp af et EU-kryptoprodukt, som er autoriseret i overensstemmelse med stk. 27, anses forbindelsen ikke for at være en sammenkobling.

38. Direkte sammenkobling eller kaskadekobling mellem et CIS, der er godkendt til at behandle oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende eller SECRET UE/EU SECRET eller tilsvarende, og et ubeskyttet eller offentligt netværk er forbudt.

B.10. ***Edb-lagringsmedier***

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

40. Edb-lagringsmedier skal genbruges, nedklassificeres eller afklassificeres i overensstemmelse med behandlingsinstrukserne.

B.11. ***Nødsituationer***

41. De særlige procedurer, der er beskrevet i det følgende, kan anvendes i en nødsituation, f.eks. under forestående eller faktiske krise-, konflikt- eller krigssituationer eller under ekstraordinære operative forhold.

42. Klassificerede oplysninger kan med den kompetente myndigheds godkendelse transmitteres ved hjælp af kryptoprodukter, der er godkendt til en lavere klassifikationsgrad, eller endog ukrypteret, 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) afsenderen og modtageren ikke har de krævede krypteringsmidler eller slet ingen krypteringsmidler, samt

b) det klassificerede materiale ikke kan sendes i tilstrækkelig god tid med andre midler.

43. Klassificerede oplysninger, der transmitteres under de i punkt 41 nævnte omstændigheder, må ikke bære nogen mærkning eller påtegning, der skiller dem ud fra oplysninger, der er uklassificeret eller kan beskyttes ved hjælp af et disponibelt kryptoprodukt. Modtagerne skal med andre midler straks underrettes om klassifikationsgraden.

44. Ved anvendelse af punkt 41 eller 42 aflægges der efterfølgende rapport til den kompetente myndighed.

SIKKERHEDSMEDDELELSE 4

FYSISK SIKKERHED

A. **INDLEDNING**

Denne sikkerhedsmeddelelse fastsætter sikkerhedsprincipperne for etablering af sikre omgivelser med henblik på korrekt behandling af fortrolige oplysninger i Europa-Parlamentet. Disse principper, herunder principperne om den tekniske sikkerhed, vil blive suppleret af behandlingsinstrukserne.

B. **SIKKERHEDSRISIKOSTYRING**

1. Risici i forhold til klassificerede oplysninger 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 sikkerhedsmeddelelse, og anvende disse foranstaltninger ifølge begrebet dybdeforsvar, jf. definitionen i sikkerhedsmeddelelse 3. Sådanne foranstaltningers effektivitet skal løbende evalueres.

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

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

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

C. **GENERELLE PRINCIPPER**

5. Klassifikationen eller graden af klassifikationen af en oplysning afgør beskyttelsesniveauet for den fysiske sikkerhed.

6. Oplysninger, der berettiger klassificering, skal mærkes og behandles i overensstemmelse hermed uanset deres fysiske form. Deres klassifikation skal klart kommunikeres til deres modtagere, enten ved en klassifikationsmærkning (hvis de gives skriftligt, det være sig på papir eller i CIS) eller ved en meddelelse (hvis informationerne gives mundtligt som f.eks. under en samtale eller en præsentation). Klassificeret materiale skal mærkes fysisk, således at dets sikkerhedsklassifikation let kan fastslås.

7. Fortrolige oplysninger må under ingen omstændigheder læses på offentlige steder, hvor de eventuelt kan blive set af en person, som ikke har »need to know«-status, f.eks. i tog, på fly, i caféer, barer og lignende. De må ikke blive efterladt i hotelsikkerhedsbokse eller på hotelværelser. De må ikke efterlades uden opsigt på offentlige steder.

D. **ANSVARSFORDELING**

8. Enheden for Klassificerede Oplysninger (CIU) er ansvarlig for den fysiske sikkerhed i forbindelse med behandlingen af fortrolige oplysninger, som er deponeret i enhedens sikrede faciliteter. CIU er ligeledes ansvarlig for forvaltningen af dens sikrede faciliteter.

9. Ansvaret for den fysiske sikkerhed for så vidt angår behandlingen af oplysninger, som er klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende, samt andre fortrolige oplysninger påhviler det respektive parlamentariske organ/hvervsindehaveren.

10. Direktoratet for Sikkerhed og Risikovurdering skal sikre den fornødne personelsikkerhedsgodkendelse med henblik på sikker behandling af fortrolige oplysninger i Europa-Parlamentet.

11. Direktoratet for Sikkerhed og Risikovurdering rådgiver om og sikrer, at ethvert oprettet eller anvendt CIS er i fuld overensstemmelse med sikkerhedsmeddelelse 3 og de respektive behandlingsinstrukser.

E. **SIKREDE FACILITETER**

12. Der kan installeres særligt sikrede faciliteter i henhold til de tekniske sikkerhedsstandarder og i overensstemmelse med de fortrolige oplysningers klassifikationsgrad som defineret i artikel 7.

13. De sikrede faciliteter skal attesteres af SAA'en og godkendes af SA'en.

F. **KONSULTATION AF FORTROLIGE OPLYSNINGER**

14. Når oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt »andre fortrolige oplysninger« er deponeret hos CIU og skal konsulteres uden for det sikrede område, sender CIU en kopi til den relevante bemyndigede tjeneste, som skal sikre, at konsultationen og behandlingen af de pågældende oplysninger sker i overensstemmelse med artikel 8, stk. 2, og artikel 10 i nærværende afgørelse, samt i overensstemmelse med de relevante behandlingsinstrukser.

15. Når oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt »andre fortrolige oplysninger« er deponeret hos et parlamentarisk organ eller en hvervsindehaver, som ikke er CIU, skal sekretariatet for det parlamentariske organ/hvervsindehaveren sikre, at konsultationen og behandlingen af de pågældende oplysninger sker i overensstemmelse med artikel 7, stk. 3, artikel 8, stk. 1, 2 og 4, artikel 9, stk. 3, 4 og 5, artikel 10, stk. 2-6, og artikel 11 i nærværende afgørelse samt i overensstemmelse med de relevante behandlingsinstrukser.

16. Når oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende skal konsulteres inden for det sikrede område, sikrer CIU, at konsultationen og behandlingen af de pågældende oplysninger sker i overensstemmelse med artikel 9 og 10 i nærværende afgørelse samt i overensstemmelse med de relevante behandlingsinstrukser.

G. **TEKNISK SIKKERHED**

17. Ansvaret for de tekniske sikkerhedsforanstaltninger påhviler SAA'en, som skal fastsætte i de relevante behandlingsinstrukser, hvilke specifikke tekniske sikkerhedsforanstaltninger der skal anvendes.

18. De sikre læseværelser, der anvendes til konsultation af oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt »andre fortrolige oplysninger« skal overholde de specifikke tekniske sikkerhedsforanstaltninger, som er fastsat i behandlingsinstrukserne.

19. Det sikrede område skal omfatte følgende faciliteter:

a) et sikkerhedsadgangskontrolrum (SAS), som skal installeres i overensstemmelse med de tekniske sikkerhedsforanstaltninger fastsat i behandlingsinstrukserne. Adgang til denne facilitet skal registreres. Sikkerhedsadgangskontrolrummet skal anvende høje standarder for så vidt angår identificering af personer med adgang, videoregistrering, og sikre områder til deponering af personlige ejendele, som ikke er tilladte i de sikrede værelser (telefoner, kuglepenne osv.)

b) et kommunikationsrum til transmission og modtagelse af klassificerede oplysninger, herunder krypterede klassificerede oplysninger, i overensstemmelse med sikkerhedsmeddelelse 3 og de respektive behandlingsinstrukser

c) et sikkert arkiv, hvor godkendte og autoriserede beholdere skal anvendes særskilt til oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL og/eller SECRET EU/EU SECRET eller tilsvarende. Oplysninger klassificeret på niveau TRES SECRET UE/EU TOP SECRET eller tilsvarende skal placeres i et separat rum i en særlig autoriseret beholder. Det eneste yderligere udstyr, som er tilladt i dette separate rum, er et arbejdsbord til CIU's administration af arkivet

d) et registreringsrum, som skal være forsynet med de nødvendige redskaber for at sikre, at registreringen kan ske på papir eller elektronisk, og dermed med de nødvendige sikrede faciliteter til at installere det passende CIS. Kun registreringsrummet må indeholde godkendte og akkrediterede reproduktionsapparater (til at lave kopier i papirform eller i elektronisk form). Behandlingsinstrukserne præciserer, hvilke reproduktionsapparater der er godkendte og akkrediterede. Registreringsrummet skal ligeledes stille de nødvendige akkrediterede materialer, der skal lagres og behandles, til rådighed til brug for mærkning, kopiering og bortskaffelse af klassificerede oplysninger i fysisk form, opdelt efter klassifikationsgrad. Alt akkrediteret udstyr skal defineres af CIU og akkrediteres af SAA'en i overensstemmelse med anbefalingen fra den operative informationssikringsmyndighed (IAOA). Registerrummet skal ligeledes udstyres med et akkrediteret destruktionsapparat godkendt til den højeste klassifikationsgrad som beskrevet i behandlingsinstrukserne. Oversættelse af oplysninger, som er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende, skal finde sted i registreringsrummet i et egnet akkrediteret system. Registreringsrummet skal udstyres med en arbejdsplads til op til to oversættere ad gangen og for samme dokument. Der skal være en ansat fra CIU til stede i registreringsrummet

e) et læseværelse til individuel konsultation af klassificerede oplysninger for behørigt bemyndigede personer. Læseværelset skal have tilstrækkelig plads til to personer, herunder en ansat fra CIU, som skal være til stede under hele konsultationen. Sikkerhedsniveauet for dette værelse skal være egnet til konsultation af oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET. Læseværelset kan, når det er nødvendigt, eventuelt udstyres med Tempestudstyr med henblik på elektronisk konsultation i overensstemmelse med klassifikationsgraden for de pågældende oplysninger

f) et mødeværelse, som skal kunne rumme op til 25 personer med henblik på drøftelse af oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET eller tilsvarende. Mødeværelset skal stille de nødvendige teknisk sikre og godkendte faciliteter til rådighed for tolkning til og fra op til to sprog. Når værelset ikke anvendes til møder, kan det ligeledes anvendes som et yderligere læseværelse til individuel konsultation. CIU kan i ekstraordinære tilfælde tillade mere end én bemyndiget person at konsultere klassificerede oplysninger, forudsat graden af sikkerhedsgodkendelse og »need to know«-status er den samme for begge personer i værelset. Højst fire personer må få adgang til konsultation af klassificerede oplysninger på samme tid. Tilstedeværelsen af tjenestemænd fra CIU skal øges

g) sikrede teknikrum til opbevaring af alt teknisk udstyr, som er tilknyttet sikkerheden for det samlede sikrede område og de sikrede it-servere.

20. Det sikrede område skal overholde de gældende internationale sikkerhedsstandarder og godkendes af Direktoratet for Sikkerhed og Risikovurdering. Det sikrede område skal være forsynet med følgende minimum af sikkerhedsteknisk udstyr:

a) alarm og overvågningssystemer

b) sikkerhedsudstyr og nødsystemer (to-vejs advarselssystem)

c) CCTV-system

d) system til afsløring af indtrængen

e) adgangskontrol (herunder et biometrisk sikkerhedssystem)

f) containere

g) garderobeskabe

h) antielektromagnetisk beskyttelse.

21. SAA kan tilføje yderligere tekniske sikkerhedsforanstaltninger, der er nødvendige, i tæt samarbejde med CIU og efter SA's godkendelse.

22. Infrastrukturudstyret kan eventuelt forbindes med det generelle styringssystem i den bygning, hvor det sikrede område befinder sig. Det sikkerhedsudstyr, som anvendes til adgangskontrol og til CIS skal imidlertid være uafhængigt af ethvert andet system af en sådan art, som findes i Europa-Parlamentet.

H. **INSPEKTION AF DET SIKREDE OMRÅDE**

23. Inspektioner af det sikrede område skal gennemføres af SAA regelmæssigt samt på anmodning af CIU.

24. SAA udarbejder og ajourfører en tjekliste til sikkerhedsinspektioner over det, der skal kontrolleres under en inspektion i overensstemmelse med behandlingsinstrukserne.

I. **TRANSPORT AF FORTROLIGE OPLYSNINGER**

25. Fortrolige oplysninger skal transporteres tildækket og uden nogen påtegning, som angiver indholdets fortrolige karakter, i overensstemmelse med behandlingsinstrukserne.

26. Kun kontorbetjente eller ansatte med den nødvendige grad af sikkerhedsgodkendelse må transportere oplysninger, der er klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende.

27. Fortrolige oplysninger må kun forsendes ved hjælp af ekstern post eller håndholdt transport uden for en bygning i overensstemmelse med betingelserne i behandlingsinstrukserne.

28. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende må aldrig sendes via e-mail eller fax, end ikke, hvis der er installeret et system for sikre e-mails eller en kryptofaxmaskine. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende og andre fortrolige oplysninger må godt sendes via e-mail eller fax, hvis der anvendes et godkendt krypteringssystem.

J. **OPBEVARING AF FORTROLIGE OPLYSNINGER**

29. Klassifikationen eller graden af klassifikation af en oplysning afgør beskyttelsesniveauet for den pågældende oplysning for så vidt angår opbevaring af oplysningen. Den skal opbevares ved hjælp af det udstyr, som er godkendt til dette formål i overensstemmelse med behandlingsinstrukserne.

30. Oplysninger, der er klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt »andre fortrolige oplysninger«:

a) skal opbevares i et låst stålskab af standardmodel på et kontor eller inden for et arbejdsområde, når de ikke bliver brugt

b) må ikke efterlades uden opsyn, medmindre de er forsvarligt opbevaret under lås

c) må ikke efterlades på en skranke, et skrivebord eller på en måde, som gør det muligt, at oplysningerne kan læses eller fjernes af ikke-bemyndigede personer, f.eks. besøgende, rengørings- eller vedligeholdelsespersonale

d) må ikke vises til eller drøftes med ikke-bemyndigede personer.

31. Oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED eller tilsvarende samt »andre fortrolige oplysninger« skal opbevares i sekretariatet for det berørte parlamentariske organ/hvervsindehaveren eller CIU i overensstemmelse med behandlingsinstrukserne.

32. Oplysninger klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIEL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller tilsvarende

a) skal opbevares i det sikrede område i en sikkerhedscontainer eller i et bokslokale. Oplysningerne kan under ekstraordinære omstændigheder, f.eks. hvis CIU er lukket, opbevares i et godkendt og autoriseret pengeskab hos sikkerhedstjenesten

b) må ikke på noget tidspunkt efterlades uden opsyn inden for det sikrede område uden først at være blevet låst inde i et godkendt pengeskab (også for meget korte fravær)

c) må ikke efterlades på en skranke eller et skrivebord på en måde, som gør det muligt, at oplysningerne kan læses eller fjernes af en ikke-bemyndiget person, uanset om den ansvarlige person fra CIU forbliver i rummet.

Når et dokument indeholdende klassificerede oplysninger udarbejdes i elektronisk form inden for det sikrede område, skal computeren låses og skærmen gøres utilgængelig, hvis udstederen eller den ansvarlige person fra CIU forlader rummet (også for meget korte fravær). En automatisk sikkerhedslås, som afbryder efter få minutter, anses ikke for at være en tilstrækkelig sikkerhedsforanstaltning.

SIKKERHEDSMEDDELELSE 5

INDUSTRIEL SIKKERHED

A. **INDLEDNING**

1. Denne sikkerhedsmeddelelse vedrører udelukkende klassificerede oplysninger.

2. Den indeholder bestemmelser for gennemførelsen af de fælles minimumsstandarder, der er fastlagt i bilag I, del 1, til denne afgørelse.

3. Ved industriel sikkerhed forstås anvendelse af foranstaltninger for at sikre, at kontrahenter eller underkontrahenter beskytter klassificerede oplysninger under forhandlingerne forud for indgåelsen af en kontrakt og under hele livscyklussen for klassificerede kontrakter. Sådanne kontrakter må ikke indebære adgang til oplysninger klassificeret på niveau TRÈS SECRET UE/EU TOP SECRET.

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

B. **SIKKERHEDSELEMENTER I EN KLASSIFICERET KONTRAKT**

B.1. ***Sikkerhedsklassifikationsvejledning (SCG)***

5. Inden der iværksættes et udbud eller tildeles en klassificeret kontrakt, skal Europa-Parlamentet som kontraherende myndighed fastsætte sikkerhedsklassifikationsgraden for oplysninger, som skal videregives til bydende og kontrahenter, samt sikkerhedsklassifikationsgraden for oplysninger, som kontrahenten skal udarbejde. Med henblik herpå udarbejder det en sikkerhedsklassifikationsvejledning (SCG), der skal anvendes ved opfyldelsen af kontrakten.

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

a) ved udarbejdelsen af en SCG skal Europa-Parlamentet tage hensyn til alle relevante sikkerhedsaspekter, herunder den sikkerhedsklassifikationsgrad, der er tildelt oplysninger, som udstederen af oplysningerne har videregivet og godkendt til brug for kontrakten

b) kontraktens overordnede klassifikationsgrad må ikke være lavere end den højeste klassifikationsgrad for dens enkelte elementer

B.2. ***Særlige sikkerhedsbetingelser (SAL)***

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

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

B.3. ***Program-/projektsikkerhedsinstruktion (PSI)***

9. Afhængigt af omfanget af programmer eller projekter, der kræver adgang til eller behandling eller opbevaring af EUCI, kan den kontraherende myndighed, der er udpeget til at forvalte det pågældende program eller projekt, udarbejde specifikke program-/projektsikkerhedsinstruktioner (PSI).

C. **SIKKERHEDSGODKENDELSE AF EN FACILITET (FSC)**

10. En FSC meddeles af en medlemsstats NSA eller anden kompetent sikkerhedsmyndighed som angivelse af, at en industrivirksomhed eller anden enhed i overensstemmelse med nationale love og bestemmelser er i stand til at sikkerhedsbeskytte EUCI med klassifikation på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET eller tilsvarende inden for sine faciliteter. Bevis for meddelelse af FSC skal forelægges for Europa-Parlamentet som kontraherende myndighed, inden en kontrahent eller underkontrahent eller en potentiel kontrahent eller underkontrahent kan få rådighed over eller tildeles adgang til EUCI.

11. En FSC skal

a) evaluere industrivirksomhedens eller en anden enheds integritet

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

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

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

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

12. Når det er relevant, skal Europa-Parlamentet som kontraherende myndighed underrette den relevante NSA eller anden kompetent sikkerhedsmyndighed om, at der er behov for en FSC i perioden forud for indgåelse af en kontrakt eller med henblik på opfyldelsen af en kontrakt. En FSC eller en sikkerhedsgodkendelse af personale (PSC) er påkrævet i perioden forud for indgåelsen af en kontrakt, hvis oplysninger, der er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal videregives i løbet af udbudsproceduren.

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

14. Den kompetente sikkerhedsmyndighed, der har udstedt en FSC, skal underrette Europa-Parlamentet om alle ændringer, der berører FSC'en. I tilfælde af en underkontrakt skal den kompetente myndighed underrettes herom.

15. Hvis den relevante NSA eller anden kompetent sikkerhedsmyndighed trækker en FSC tilbage, anses det for tilstrækkelig grund til, at Europa-Parlamentet som kontraherende myndighed kan ophæve en klassificeret kontrakt eller udelukke en bydende fra udvælgelsen.

D. **KLASSIFICEREDE KONTRAKTER OG UNDERKONTRAKTER**

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

17. Når der er tildelt en klassificeret kontrakt eller underkontrakt, underretter Europa-Parlamentet som kontraherende myndighed kontrahentens og/eller underkontrahentens NSA eller anden kompetent sikkerhedsmyndighed om sikkerhedsbestemmelserne for den klassificerede kontrakt.

18. Ved ophævelse af sådanne kontrakter, underretter Europa-Parlamentet som kontraherende myndighed (og/eller den kompetente sikkerhedsmyndighed i tilfælde af en underkontrakt, alt efter hvad der er hensigtsmæssigt,) straks NSA'en eller anden kompetent sikkerhedsmyndighed i den medlemsstat, hvor kontrahenten eller underkontrahenten er registreret.

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

20. Særlige bestemmelser for bortskaffelse af klassificerede oplysninger under opfyldelsen af kontrakten eller ved dens ophævelse fastsættes i SAL.

21. Er kontrahenten eller underkontrahenten autoriseret til at beholde klassificerede oplysninger efter kontraktens ophævelse, skal minimumsstandarderne i denne afgørelse fortsat anvendes, og kontrahenten eller underkontrahenten skal beskytte de klassificerede oplysningers fortrolighed.

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

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

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

25. For så vidt angår klassificerede oplysninger, der udarbejdes eller håndteres af kontrahenten eller underkontrahenten, varetager den kontraherende myndighed udsteders rettigheder.

E. **BESØG I FORBINDELSE MED KLASSIFICEREDE KONTRAKTER**

26. Hvis Europa-Parlamentet, kontrahenter eller underkontrahenter har behov for adgang til oplysninger, der er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, i hinandens lokaler med henblik på opfyldelse af en klassificeret kontrakt, skal der tilrettelægges besøg i samråd med de pågældende NSA'er eller anden berørt kompetent sikkerhedsmyndighed. I forbindelse med specifikke projekter kan NSA'erne dog også aftale en procedure, hvorved sådanne besøg kan tilrettelægges direkte.

27. Alle besøgende skal være i besiddelse af en relevant PSC og have »need to know«-status med henblik på adgang til klassificerede oplysninger vedrørende kontrakten med Europa-Parlamentet.

28. Besøgende kan kun få adgang til klassificerede oplysninger, der har forbindelse med besøgets formål.

F. **TRANSMISSION OG TRANSPORT AF KLASSIFICEREDE OPLYSNINGER**

29. For så vidt angår elektronisk transmission af klassificerede oplysninger anvendes de relevante bestemmelser i sikkerhedsmeddelelse 3.

30. For så vidt angår transport af klassificerede oplysninger anvendes de relevante bestemmelser i sikkerhedsmeddelelse 4 og de relevante behandlingsinstrukser.

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

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

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

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

d) forud for enhver grænseoverskridende transport af materiale, der er klassificeret på niveau CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET eller tilsvarende, skal afsenderen udarbejde en transportplan, som skal godkendes af generalsekretæren

e) transporten gennemføres så vidt muligt fra et givet afgangssted til et givet ankomststed og afsluttes så hurtigt, som forholdene tillader

f) ruterne bør så vidt muligt kun gå gennem medlemsstaters områder.

G. **VIDEREGIVELSE AF KLASSIFICEREDE OPLYSNINGER TIL KONTRAHENTER I TREDJELANDE**

32. Klassificerede oplysninger skal videregives til kontrahenter og underkontrahenter i tredjelande i overensstemmelse med de sikkerhedsforanstaltninger, der er aftalt mellem Europa-Parlamentet som kontraherende myndighed og det pågældende tredjeland, hvor kontrahenten er registreret.

H. **BEHANDLING OG OPBEVARING AF OPLYSNINGER KLASSICERET PÅ NIVEAU RESTREINT UE/EU RESTRICTED**

33. Europa-Parlamentet har som kontraherende myndighed ret til, eventuelt i samarbejde med den berørte medlemsstats NSA, at besøge kontrahenters/underkontrahenters faciliteter på grundlag af kontraktbestemmelser for at kontrollere, at de relevante sikkerhedsforanstaltninger til beskyttelse af EUCI, der er klassificeret RESTREINT UE/EU RESTRICTED, er iværksat som krævet ifølge kontrakten.

34. I det omfang, det er nødvendigt i henhold til nationale love og bestemmelser, underretter Europa-Parlamentet som kontraherende myndighed NSA'erne eller anden kompetent sikkerhedsmyndighed om kontrakter eller underkontrakter, der indeholder oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED.

35. En FSC eller en PSC til kontrahenter eller underkontrahenter og deres personale er ikke påkrævet for kontrakter, der tildeles af Europa-Parlamentet og indeholder oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED.

36. Europa-Parlamentet undersøger som kontraherende myndighed svarene på indkaldelse af bud vedrørende kontrakter, der kræver adgang til oplysninger klassificeret på niveau RESTREINT UE/EU RESTRICTED, uanset de krav med hensyn til FSC eller PSC, der måtte findes i nationale love og bestemmelser.

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

38. Hvis en kontrakt indebærer behandling af oplysninger klassificeres på niveau RESTREINT UE/EU RESTRICTED i et kommunikations- og informationssystem, som drives af en kontrahent, sikrer Europa-Parlamentet som kontraherende myndighed, at kontrakten samt eventuelle underkontrakter nærmere beskriver de nødvendige tekniske og administrative krav for akkreditering af kommunikations- og informationssystemet, som svarer til den vurderede risiko, under hensyntagen til alle relevante faktorer. Anvendelsesområdet for kommunikations- og informationssystemet skal aftales mellem den kontraherende myndighed og den relevante NSA.

SIKKERHEDSMEDDELELSE 6

BRUD PÅ SIKKERHEDEN, TAB ELLER KOMPROMITTERING AF FORTROLIGE OPLYSNINGER

1. Ved et brud på sikkerheden forstås resultatet af en persons handling eller forsømmelse, som kan skade eller føre til kompromittering af fortrolige oplysninger.

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

3. Kompromittering af fortrolige oplysninger kan ske som følge af skødesløse eller uagtsomme handlinger eller mangel på diskretion, samt hvis Unionen gøres til genstand for spionage eller undergravende virksomhed.

4. Hvis generalsekretæren opdager eller oplyses om et tilfælde, hvor der er bevis for eller mistanke om brud på sikkerheden, tab eller kompromittering af fortrolige oplysninger, skal generalsekretæren

a) fastslå sagens omstændigheder

b) vurdere og begrænse den forvoldte skade

c) træffe foranstaltninger til at forhindre gentagelser

d) underrette den kompetente myndighed om den tredjemand eller medlemsstat, som har udfærdiget eller videresendt de fortrolige oplysninger.

Når et medlem af Europa-Parlamentet er indblandet, handler generalsekretæren for Europa-Parlamentet sammen med Europa-Parlamentets formand.

Hvis oplysningen stammer fra andre EU-institutioner, handler generalsekretæren i overensstemmelse med de relevante sikkerhedsforanstaltninger for klassificerede oplysninger og de regler, som er fastsat i rammeaftalen med Kommissionen eller den interinstitutionelle aftale med Rådet.

5. Alle personer, der skal håndtere fortrolige oplysninger, skal gøres grundig bekendt med sikkerhedsprocedurer og den risiko, der er forbundet med indiskrete samtaler og deres forbindelser med medierne, og skal om nødvendigt underskrive en erklæring om, at de ikke vil videregive indholdet af fortrolige oplysninger til tredjemand, at de vil overholde deres forpligtelser med hensyn til at beskytte klassificerede oplysninger, og at de er klar over konsekvenserne af at undlade dette. Adgang til eller brug af klassificerede oplysninger af en person, som ikke er blevet gjort bekendt med sine forpligtelser eller har underskrevet den pågældende erklæring, betragtes som et brud på sikkerheden.

6. Medlemmer af Europa-Parlamentet, Europa-Parlamentets tjenestemænd samt andre ansatte, der arbejder for politiske grupper, eller kontrahenter, skal omgående underrette generalsekretæren om ethvert brud på sikkerheden, tab eller kompromittering af fortrolige oplysninger, som de får kendskab til.

7. Enhver person, der gør sig skyldig i kompromittering af fortrolige oplysninger, pålægges disciplinære sanktioner i overensstemmelse med de relevante regler og bestemmelser. Disciplinære sanktioner udelukker ikke, at den pågældende retsforfølges i overensstemmelse med gældende love.

8. Uden at det berører andre retlige foranstaltninger fører brud på reglerne begået af Europa-Parlamentets tjenestemænd og andre ansatte, der arbejder for politiske grupper, til anvendelse af procedurerne og sanktionerne i afsnit VI i personalevedtægten.

9. Uden at det berører andre retlige foranstaltninger, behandles brud på reglerne begået af Europa-Parlamentets medlemmer i overensstemmelse med Europa-Parlamentets forretningsordens artikel 9, stk. 2, artikel 152, 153 og 154.