IV

(Oplysninger)

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

EUROPA-PARLAMENTET

EUROPA-PARLAMENTETS PRÆSIDIUMS AFGØRELSE

af 6. juni 2011

om regler om Europa-Parlamentets behandling af fortrolige oplysninger

(2011/C 190/02)

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«), er en revision af Præsidiets afgørelse af 13. november 2006 om regler om administrativ behandling af fortrolige dokumenter blevet nødvendig.

(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 artikel 15 i traktaten om Den Europæiske Unions funktionsmåde (TEUF) og Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter [2].

(5) Reglerne i denne afgørelse berører ikke artikel 16 i TEUF og Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger [3] —

VEDTAGET FØLGENDE AFGØRELSE:

Artikel 1

Formål

Denne afgørelse regulerer Europa-Parlamentets oprettelse, modtagelse, fremsendelse og opbevaring af fortrolige oplysninger med henblik på at sikre en passende beskyttelse af deres fortrolige karakter. Den gennemfører navnlig bilag 2 til Rammeaftalen.

[1] EUT L 304 af 20.11.2010, s. 47.

[2] EFT L 145 af 31.5.2001, s. 43.

[3] EFT L 8 af 12.1.2001, s. 1.

Artikel 2

Definitioner

I denne afgørelse finder følgende definitioner anvendelse:

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

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

c) Ved »EU-klassificerede oplysninger« 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 og agenturer oprettet med hjemmel i traktaterne eller er modtaget fra medlemsstater, tredjelande eller internationale organisationer. I den forbindelse er:

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

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

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

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

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

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

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

h) Ved »godkendelse« forstås en beslutning (beslutning om sikkerhedsgodkendelse) truffet af formanden, hvis den vedrører medlemmer af Europa-Parlamentet, og af generalsekretæren, hvis den vedrører Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper, om at give en enkeltperson adgang til EU-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.

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

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

k) Ved »ophavsmand« forstås den behørigt bemyndigede ophavsmand til EU-klassificerede oplysninger eller andre fortrolige oplysninger.

l) Ved »sikkerhedsmeddelelser« forstås tekniske gennemførelsesbestemmelser som fastlagt i bilag II ([1]).

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, som skal have 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 ophavsmanden til de pågældende oplysninger i sikkerhedsmeddelelserne.

Europa-Parlamentets behandling af fortrolige oplysninger ved hjælp af automatiske informationssystemer gennemføres i overensstemmelse med begrebet informationssikring og sikkerhedsmeddelelserne.

([1]) Bilag skal vedtages.

3. Europa-Parlamentets medlemmer kan få adgang til klassificerede oplysninger op til og med niveauet CONFIDENTIEL UE/EU CONFIDENTIAL uden sikkerhedsgodkendelse. I forbindelse med oplysninger, der er klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL, skal de underskrive en erklæring på tro og love om, at de ikke vil videregive oplysningernes indhold til tredjemand. Medlemmer kan kun få adgang til oplysninger, der er klassificeret højere end CONFIDENTIEL UE/EU CONFIDENTIAL, hvis de har den fornødne sikkerhedsgodkendelse.

4. 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 over RESTREINT UE/EU RESTRICTED, hvis de har den fornødne sikkerhedsgodkendelse.

Artikel 4

Oprettelse 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 ophavsmanden det passende klassificeringsniveau i overensstemmelse med de internationale standarder og definitioner i bilag I. Ophavsmanden bestemmer som hovedregel også, hvilke adressater der skal kunne få adgang til oplysningerne, i forhold til klassificeringsniveauet. Disse oplysninger gives til Kontoret for Fortrolige Oplysninger, når dokumentet indleveres til kontoret.

3. Fortrolige oplysninger, der er omfattet af tavshedspligt, behandles i overensstemmelse med instrukserne i sikkerhedsmeddelelserne.

Artikel 5

Europa-Parlamentets modtagelse af fortrolige oplysninger

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

— EU-klassificerede oplysninger klassificeret som RESTREINT UE/EU RESTRICTED og andre fortrolige oplysninger, til sekretariatet for det berørte parlamentariske organ/den hvervsindehaver, der har indgivet anmodningen herom

— EU-klassificerede oplysninger klassificeret som CONFIDENTIEL UE/EU CONFIDENTIEL og derover, til Kontoret for Fortrolige Oplysninger.

2. Sekretariatet for det parlamentariske organ/den hvervsindehaver, der modtog oplysningerne, eller Kontoret for Fortrolige Oplysninger sørger for fortrolige oplysningers registrering, opbevaring og sporbarhed.

3. Er der tale om fortrolige oplysninger meddelt af Kommissionen, jf. Rammeaftalen, indleveres de nærmere regler for adgang til oplysningerne og bevarelse af deres fortrolige karakter, der er aftalt, jf. bilag II, punkt 3.2, i Rammeaftalen (fastlagt ved fælles overenskomst og vedrørende de personer, fortrolige oplysninger må udleveres til, proceduren for adgang til oplysninger, dvs. et sikkert læseværelse, møde for lukkede døre samt andre forhold), sammen med de fortrolige oplysninger til sekretariatet for det parlamentariske organ/hvervsindehaveren eller til Kontoret for Fortrolige Oplysninger, når oplysningerne er klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL eller derover.

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. EU-klassificerede oplysninger klassificeret som TRÈS SECRET UE/EU TOP SECRET fremsendes til Europa-Parlamentet i overensstemmelse med yderligere nærmere regler, der aftales mellem det parlamentariske organ/den hvervsindehaver, der har indgivet anmodningen om oplysningerne, og den EU-institution eller medlemsstat, der modtager oplysningerne. Formandskonferencen nedsætter et tilsynsudvalg. Det skal sikre et højt beskyttelsesniveau svarende til klassifikationsgraden.

Artikel 6

Europa-Parlamentets videregivelse af EU-klassificerede oplysninger til tredjemand

Europa-Parlamentet kan, med ophavsmandens samtykke, videregive EU-klassificerede oplysninger til andre institutioner, organer, kontorer eller agenturer eller til medlemsstater 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 EU-klassificerede oplysninger.

Artikel 7

Opbevaring og konsultation af fortrolige oplysninger i sikrede områder (sikkert læseværelse)

1. Sikre læseværelser skal give mulighed for sikker opbevaring, og der må ikke være fotokopimaskiner, telefoner, fax, scanner eller anden teknik til reproduktion eller videresendelse af dokumenter.

2. Adgang til sikre læseværelser sker på følgende betingelser:

a) Adgang er forbeholdt følgende personer:

— medlemmer af Europa-Parlamentet, Europa-Parlamentets tjenestemænd og Parlamentets øvrige ansatte, der arbejder for politiske grupper, som er behørigt identificeret i overensstemmelse med de i artikel 4, stk. 2, eller artikel 5, stk. 3, omhandlede nærmere regler

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

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

Rengøring af det sikrede område må kun finde sted under tilstedeværelse af og under tæt overvågning af en tjenestemand fra Kontoret for Fortrolige Oplysninger.

b) Personer, der ønsker at få adgang til fortrolige oplysninger, meddeler på forhånd deres navn til Kontoret for Fortrolige Oplysninger. Kontoret for Fortrolige Oplysninger kontrollerer identiteten af personer, der indgiver anmodning om at konsultere disse oplysninger, og undersøger om nødvendigt, om den pågældende har den fornødne sikkerhedsgodkendelse og er godkendt dertil, i overensstemmelse med de i artikel 4, stk. 2, eller artikel 5, stk. 3, omhandlede nærmere regler.

c) Kontoret for Fortrolige Oplysninger kan nægte enhver person, som ikke er godkendt dertil i henhold til litra a) og b), adgang til værelset. Enhver indsigelse mod den af Kontoret for Fortrolige Oplysninger trufne afgørelse indbringes for formanden, når der er tale om medlemmer af Europa-Parlamentet, og for generalsekretæren i andre tilfælde.

3. Konsultation af fortrolige oplysninger i det sikre læseværelse sker på følgende betingelser:

a) Personer, som har fået tilladelse til at konsultere oplysninger og har indgivet den i stk. 2, litra b, omhandlede anmodning, skal møde personligt i Kontoret for Fortrolige Oplysninger.

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 Kontoret for Fortrolige Oplysninger konsultere oplysninger i det sikre læseværelse.

Den pågældende tjenestemand oplyser den person, der har fået tilladelsen, om de dermed forbundne forpligtelser og anmoder den pågældende om at underskriver en erklæring på tro og love om, at indholdet af oplysningerne ikke vil blive videregivet til tredjemand.

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

c) Før en person får tilladelse til at forlade det sikre læseværelse, kontrollerer den i litra a) omhandlede ansvarlige tjenestemand fra Kontoret for Fortrolige Oplysninger, at de konsulterede fortrolige oplysninger stadig er til stede, intakte og fuldstændige.

4. Ved overtrædelse af ovenstående regler underretter den ansvarlige tjenestemand fra Kontoret for Fortrolige Oplysninger generalsekretæren, der indbringer sagen for formanden, hvis der er tale om et medlem af Europa-Parlamentet.

Artikel 8

Minimumsstandarder for andre former for konsultation af fortrolige oplysninger

1. Hvad angår administrativ behandling af fortrolige oplysninger på et møde for lukkede døre sikrer sekretariatet for det parlamentariske organ/den hvervsindehaver, der er ansvarlig(t) for mødet, at

— kun de personer, der er udpeget til at deltage i mødet og har den fornødne sikkerhedsgodkendelse, får adgang til mødeværelset

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

— protokollen fra mødet ikke omtaler drøftelsen af de oplysninger, som er behandlet fortroligt

— fortrolige oplysninger, som afgives mundtligt til modtagere i Europa-Parlamentet, er omfattet af det samme beskyttelsesniveau som det, der ville finde anvendelse for skriftlige fortrolige oplysninger. Dette kan omfatte en erklæring på tro og love fra modtagerne af oplysningerne om, at de ikke vil videregive oplysningernes indhold til tredjemand.

2. Hvad angår administrativ behandling af fortrolige oplysninger foretaget af sekretariatet for det parlamentariske organ/hvervsindehaveren uden for det lukkede møde gælder følgende regler:

— Papirdokumenterne indleveres personligt til chefen for sekretariatet, som registrerer dem og kvitterer for modtagelsen

— dokumenterne opbevares under lås på sekretariatets ansvar, når de ikke bliver brugt

— medmindre andet følger af reglerne om administrativ behandling af fortrolige oplysninger på et møde for lukkede døre, jf. stk. 1, må dokumenterne under ingen omstændigheder kopieres, gemmes på et andet medium eller sendes til nogen

— kun dokumenternes adressater har adgang til disse under sekretariatets tilsyn i overensstemmelse med de i artikel 4, stk. 2, eller artikel 5, stk. 3 eller 4, nævnte nærmere regler

— sekretariatet fører en fortegnelse over de personer, der har konsulteret dokumenterne, og datoen og tidspunktet herfor. Denne fortegnelse sendes til Kontoret for Fortrolige Oplysninger med henblik på udarbejdelsen af den i artikel 12 omhandlede årsberetning.

Artikel 9

Arkivering af fortrolige oplysninger

1. Der føres et sikkert arkiveringssystem i Europa-Parlamentets lokaler.

Fortrolige oplysninger, der deponeres endeligt hos Kontoret for Fortrolige Oplysninger eller det parlamentariske organs sekretariat/hvervsindehaveren, overføres til det sikre arkiv i Kontoret for Fortrolige Oplysninger seks måneder efter den sidste konsultation og senest et år efter deponeringen.

2. Kontoret for Fortrolige Oplysninger forvalter det sikre arkiv i overensstemmelse med standardkriterier for arkivering.

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

— der gives kun tilladelse til personer, der er identificeret ved navn eller funktion i det ledsagedokument, der blev udfyldt ved deponering af dokumentet

— der skal indgives en anmodning om konsultation til Kontoret for Fortrolige Oplysninger, der sørger for overførsel af dokumentet fra arkivet til det sikre læseværelse

— procedurerne og betingelserne for konsultation af fortrolige oplysninger som fastsat i artikel 7 finder anvendelse.

Artikel 10

Nedklassificering og afklassificering af EU-klassificerede oplysninger

1. EU-klassificerede oplysninger må kun nedklassificeres eller afklassificeres med ophavsmandens tilladelse og om nødvendigt efter drøftelse med andre berørte parter. Nedklassificeringen eller afklassificeringen bekræftes skriftligt. Ophavsmanden 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.

2. Dokumenter i de sikre arkiver afklassificeres senest efter 30 år efter 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 ophavsmanden til de klassificerede oplysninger eller af det på det relevante tidspunkt ansvarlige kontor i overensstemmelse med bilag I, del 1, punkt 10.

Artikel 11

Brud på fortroligheden

1. 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. Brud på reglerne begået af medarbejdere 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«).

3. Formanden og generalsekretæren iværksætter de nødvendige undersøgelser.

Artikel 12

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

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

Artikel 13

Gældende bestemmelser og overgangsbestemmelser

1. Fortrolige oplysninger, der fandtes i Kontoret for Fortrolige Oplysninger eller i arkiverne før denne afgørelse fandt anvendelse, klassificeres automatisk som RESTREINT UE/EU RESTRICTED, medmindre ophavsmanden beslutter, at de ikke skal klassificeres, eller at give dem en højere klassifikationsgrad eller en påtegning inden for et år efter denne afgørelses ikrafttræden.

2. Hvis ophavsmanden til sådanne fortrolige oplysningerne beslutter at give dem en højere klassifikationsgrad, klassificeres dokumenterne med den lavest mulige grad af ophavsmanden eller dennes stedfortrædere i samarbejde med Kontoret for Fortrolige Oplysninger og i overensstemmelse med kriterierne i bilag I til denne afgørelse.

3. Præsidiets afgørelse af 13. november 2006 om regler om administrativ behandling af fortrolige dokumenter ophæves.

4. Præsidiets afgørelse af 24. oktober 2005, hvorved der blev givet mandat til generalsekretæren til at nedsætte et afklassificeringsudvalg og til at træffe afgørelser om afklassificering, ophæves.

Artikel 14

Ikrafttræden

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

2. Den finder anvendelse fra den 1. juli 2011.

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 minimumsstandarder for sikkerhedsbeskyttelse, som skal overholdes ikke blot af Europa-Parlamentet på alle dets tjenestesteder, men også af alle modtagere af EU-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. De suppleres af regler for 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.

Legalitetsprincippet medfører, at de gældende rammebestemmelser nøje skal iagttages ved udøvelsen af sikkerhedsfunktionerne, og at alle de krav i bestemmelserne, der finder anvendelse, skal opfyldes. Det betyder også, at ansvarsområderne vedrørende sikkerhed skal 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 betyder det, at brud på sikkerhedsbestemmelserne inden for Europa-Parlamentets ansvarsområde skal behandles i overensstemmelse med Europa-Parlamentets politik vedrørende disciplinære sanktioner.

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

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

Subsidiaritetsprincippet medfører, at sikkerheden skal tilrettelægges på det lavest mulige niveau og så nært som muligt på Europa-Parlamentets generaldirektorater og tjenester. Proportionalitetsprincippet medfører, 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 de kan forsvares på en måde, der medfører de mindst mulige forstyrrelser.

3. **Grundlaget for sikkerhedsbeskyttelse af oplysninger**

Grundlaget for en effektiv sikkerhedsbeskyttelse af oplysninger er:

a) at der i Parlamentet udpeges en Infosec-myndighed — en myndighed til sikring af informationssikkerhed — som inden for den pågældende sikkerhedsorganisation er ansvarlig for at underrette og rådgive om tekniske sikkerhedsrisici og modforholdsregler

b) at der er et nært samarbejde mellem Europa-Parlamentets ansvarlige organer og sikkerhedsorganerne ved de øvrige EU-institutioner.

4. **Principperne for informationssikkerhed**

4.1. *Formål*

Informationssikkerhedens vigtigste formål er:

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

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

c) at beskytte Europa-Parlamentets bygninger, der rummer EU-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 de nødvendige foranstaltninger for at undgå gentagelse.

4.2. *Klassifikation*

4.2.1. Der skal udvises stor omhu og eftertanke ved udvælgelsen af, hvilke oplysninger og hvilket materiale der skal sikkerhedsbeskyttes, og ved vurderingen af, hvilken grad af sikkerhedsbeskyttelse der er behov for. Det er afgørende, at klassifikationsgraden stemmer overens med den 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 skal gennemføres; der anvendes en tilsvarende klassificeringsordning ved planlægning og tilrettelæggelse af beskyttelsen mod spionage, sabotage, terrorisme og andre trusler, således at de vigtigste bygninger og områder, der rummer EU-klassificerede oplysninger, og de mest følsomme steder i disse bygninger og områder gives maksimal beskyttelse.

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. Hvis flere dokumenter med oplysninger grupperes, skal klassifikationsgraden for det samlede materiale mindst være lige så høj som den højeste af de enkelte dokumenters klassifikationsgrader. En samling af oplysninger kan dog gives en højere klassifikationsgrad 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 EU-klassificerede oplysninger, informationsbærende medier med EU-klassificerede oplysninger, andre fortrolige oplysninger, såvel som alle bygninger og områder, der rummer sådanne oplysninger, og vigtige anlæg

b) tage sigte på at identificere personer, som kan udgøre en sikkerhedsmæssig risiko for 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 (dvs. 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, uanset om oplysningerne er klassificerede eller uklassificerede.

5. **Fælles minimumsstandarder**

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

Europa-Parlamentet giver kun eksterne organer adgang til sådanne oplysninger på betingelse af, at de sikrer, at der ved behandlingen af oplysningerne iagttages bestemmelser, der i det mindste 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 for europa-parlamentets tjenestemænd og parlamentets øvrige ansatte, der arbejder for politiske grupper**

6.1. *Sikkerhedsinstruks til 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 EU-klassificerede oplysninger, inden de påbegynder arbejdet og derefter regelmæssigt, skal modtage en indgående instruks om nødvendigheden af sikkerhedsbeskyttelsen og procedurerne for gennemførelsen heraf. Sådanne personer skal skriftligt attestere, 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 til 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 det bekræftes, at medarbejderen udgør en sikkerhedsrisiko, skal den pågældende udelukkes fra eller fratages arbejdsopgaver, hvor vedkommende kan være til fare for sikkerheden.

7. **Fysisk sikkerhed**

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

7.1. *Behovet for sikkerhedsbeskyttelse*

Graden af de fysiske foranstaltninger, der skal bringes i anvendelse for at sikre beskyttelsen af EU-klassificerede oplysninger, skal stå i forhold til klassifikationsgraden samt omfanget af og truslen mod de oplysninger og det materiale, det drejer sig om. Alle, der ligger inde med EU-klassificerede oplysninger, skal følge en ensartet praksis med hensyn til klassificering af 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 EU-klassificerede oplysninger, må ikke efterlade disse uden opsigt, men skal sikre sig, at de opbevares forsvarligt, og at alle sikkerhedsanordninger er aktiveret (låse, alarmsystemer osv.). Herudover foretages der efter arbejdstids ophør kontrol af, om disse krav er opfyldt.

7.3. *Sikkerhedsbeskyttelse af bygninger*

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

Hvordan EU-klassificerede oplysninger skal beskyttes, 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 udarbejdes detaljerede planer for, hvordan klassificerede oplysninger skal beskyttes, 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 c).

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

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

Sikkerhedsangivelser må kun benyttes i forbindelse med en klassifikationsgrad.

8.2. *Påtegninger*

Det kan med en særlig påtegning 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 må ikke anvendes i stedet for en sådan.

8.3. *Anførelse af klassifikationsgrad og sikkerhedspåtegninger*

Klassifikationsgraden anføres således:

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

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

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

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

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 dokumenter med klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET, skal holdes på et minimum, og deres navne skal stå på en liste, der udarbejdes af Kontoret for Fortrolige Oplysninger.

8.4.2. Anvendelse af klassifikationsgrader

Klassificeringen af et dokument afhænger af, hvor følsomt dets indhold er, jf. definitionen i artikel 2, litra c). Det er vigtigt, at klassifikationsgrader anvendes korrekt og under udvisning af mådehold, navnlig for så vidt angår klassifikationsgraden TRÈS SECRET UE/EU TOP SECRET.

Et brev eller en følgeskrivelse klassificeres i overensstemmelse med bilagenes højeste klassifikationsgrad. Dokumentets udsteder skal klart angive, på hvilket niveau brevet eller følgeskrivelsen skal klassificeres, hvis det/den adskilles fra bilaget.

Udstederen skal ved klassificeringen af et dokument være opmærksom på ovenstående bestemmelser og bremse enhver tendens til at anvende for høj eller for lav klassifikationsgrad.

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 med ansvar for sikkerhed gennemfører regelmæssige inspektioner af sikkerhedsordningerne for beskyttelse af EU-klassificerede oplysninger og kan i denne forbindelse bistås af Kontoret for Fortrolige Oplysninger.

Europa-Parlamentets Direktorat med ansvar for sikkerhed og sikkerhedstjenesterne i andre institutioner, organer, kontorer og agenturer oprettet med hjemmel i traktaterne, der ligger inde med EU-klassificerede oplysninger, kan også aftale at gennemføre peer-evalueringer af hinandens sikkerhedsordninger til beskyttelse af EU-klassificerede oplysninger.

10. **Afklassificeringsprocedure**

10.1. Kontoret for Fortrolige Oplysninger gennemgår EU-klassificerede oplysninger og fremsætter under alle omstændigheder forslag om afklassificering til udstederen af dokumentet senest 25 år efter datoen for dets udarbejdelse. Dokumenter, der ikke er blevet afklassificeret ved første gennemgang, gennemgås igen regelmæssigt og mindst hvert femte år.

10.2. Udover at finde anvendelse for dokumenter, der faktisk befinder sig i de sikre arkiver og er blevet behørigt klassificeret, kan afklassificeringsproceduren endvidere finde anvendelse på andre fortrolige oplysninger, der befinder sig i de sikre arkiver eller Europa-Parlaments Arkiv- og Dokumentationscenter (CARDOC).

10.3. På vegne af udstederen er Kontoret for Fortrolige Oplysninger ansvarlig for at underrette dokumentets modtagere om ændringen af klassificeringen, 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 påtegninger på dokumentet.

10.5. Den oprindelige klassifikation for oven og for neden på hver enkelt side overstreges. Dokumentets første side stemples og forsynes med Kontoret for Fortrolige Oplysningers reference.

10.6. Det afklassificerede dokuments tekst 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 Kontoret for Fortrolige Oplysninger sig med den pågældende tredjemand, før det iværksætter en afklassificering. Tredjemanden har otte uger til at fremsætte sine bemærkninger

b) For så vidt angår undtagelsen vedrørende privatlivets fred og den enkeltes integritet tages ved en afklassificeringsprocedure navnlig hensyn til, at den berørte har givet samtykke, at det er umuligt at identificere den berørte person, og at den pågældende person ikke længere er i live

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 denne offentliggørelse til at fremsætte eventuelle bemærkninger.

DEL 2

SIKKERHEDSGODKENDELSE

11. **Sikkerhedsgodkendelse af medlemmer**

11.1. I kraft af Europa-Parlamentets prærogativer og beføjelser kan dets medlemmer gives adgang til EU-klasssificerede oplysninger til og med graden CONFIDENTIEL UE/EU CONFIDENTIEL. I forbindelse med oplysninger klassificeret som CONFIDENTIEL UE/EU CONFIDENTIAL skal de underskrive en erklæring på tro og love om, at de ikke vil videregive indholdet af de pågældende oplysninger til tredjemand.

11.2. For at få adgang til oplysninger klassificeret som TRÈS SECRET UE/EU TOP SECRET, eller SECRET UE/EU SECRET skal medlemmerne af Europa-Parlamentet først godkendes til den pågældende klassifikationsgrad efter proceduren i punkt 11.3 og 11.4.

11.3. Kun de af Europa-Parlamentets medlemmer, der er blevet sikkerhedsundersøgt af medlemsstaternes 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 meddeler godkendelsen 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 med ansvar for sikkerhed 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 kan inddrage godkendelsen, hvis vedkommende finder, at der er grund hertil. 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, og 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 klassifikationsniveauet for de oplysninger, som det pågældende medlem af Europa-Parlamentet vil få kendskab til, så de kan foretage sikkerhedsundersøgelsen.

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

11.12. Afgiver medlemsstaternes nationale myndigheder positiv udtalelse, kan formanden godkende det pågældende medlem af Europa-Parlamentet.

11.13. Afgiver de nationale myndigheder 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 vedkommende rette henvendelse til de kompetente nationale myndigheder 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 instrukser om beskyttelse af klassificerede oplysninger og om, hvordan de skal beskyttes. Det godkendte medlem underskriver en erklæring som bekræftelse på at have modtaget disse instrukser.

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 de kompetente nationale myndigheder på forhånd er blevet underrettet, og disse ikke har fremsat bemærkninger inden for en måned. Sådanne midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret som TRÈS SECRET UE/EU TOP SECRET.

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 til sådanne oplysninger.

12.2. For at få adgang til oplysninger, der er klassificeret som TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET og CONFIDENTIEL UE/EU CONFIDENTIAL, skal de i punkt 12.1 omhandlede medarbejdere 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 meddeler godkendelsen efter at have indhentet udtalelse fra medlemsstaternes kompetente nationale myndigheder på grundlag af den sikkerhedsundersøgelse, der er foretaget i henhold til punkt 12.8 til 12.13.

12.5. Europa-Parlamentets Direktorat med ansvar for sikkerhed 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 som omhandlet i punkt 12.8.

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 kan inddrage godkendelsen, hvis vedkommende finder, at der er grund hertil. Inddrages godkendelsen, underrettes den pågældende af Europa-Parlamentets tjenestemænd eller øvrige af Parlamentets ansatte, der arbejder for de politiske grupper, og den pågældende kan anmode om at måtte fremsætte sine bemærkninger over for generalsekretæren, inden inddragelsen får virkning, og de nationale myndigheder.

12.8. Sikkerhedsundersøgelsen foretages med den berørte persons medvirken 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 som CONFIDENTIEL UE/EU CONFIDENTIAL eller højere.

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 arten af og klassifikationsniveauet for de oplysninger, som den pågældende person vil få kendskab til, så de 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 de kompetente nationale myndigheder foretagne sikkerhedsundersøgelses forløb og dens resultater.

12.12. Afgiver medlemsstaternes nationale myndigheder positiv udtalelse, kan generalsekretæren godkende den pågældende person.

12.13. Afgiver de nationale myndigheder 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 de nationale myndigheder 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. Den pågældende tjenestemand eller 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 de kompetente nationale myndigheder på forhånd er blevet underrettet, og disse ikke har fremsat bemærkninger inden for en måned. Sådanne midlertidige godkendelser giver ikke adgang til oplysninger, der er klassificeret som TRÈS SECRET UE/EU TOP SECRET.