IV

(Upplysningar)

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER OCH ORGAN

EUROPAPARLAMENTET

BESLUT AV EUROPAPARLAMENTETS PRESIDIUM

av den 6 juni 2011

om bestämmelserna för Europaparlamentets hantering av sekretessbelagda uppgifter

(2011/C 190/02)

EUROPAPARLAMENTETS PRESIDIUM HAR FATTAT DETTA BESLUT

med beaktande av artikel 23.12 i Europaparlamentets arbetsordning,

och av följande skäl:

(1) Mot bakgrund av det nya ramavtalet av den 20 oktober 2010 om förbindelserna mellan Europaparlamentet och Europeiska kommissionen [1] *(ramavtalet)* gör det nödvändigt att se över presidiets beslut av den 13 november 2006 om bestämmelserna för förvaltningens hantering av sekretessbelagda handlingar.

(2) Lissabonfördraget ger Europaparlamentet nya befogenheter. För att parlamentets verksamhet ska kunna utvecklas på de områden där det krävs en viss sekretess måste det fastställas grundläggande principer, miniminormer för säkerhet och lämpliga bestämmelser för Europaparlamentets hantering av sekretessbelagda uppgifter.

(3) Syftet med bestämmelserna i detta beslut är att garantera motsvarande skyddsnormer och överensstämmelse med de bestämmelser som har antagits av andra institutioner, organ och byråer som har upprättats genom eller på grundval av fördragen eller av medlemsstaterna för att Europeiska unionens beslutsprocess ska kunna fungera på ett smidigt sätt.

(4) Bestämmelserna i detta beslut antas utan att det påverkar artikel 15 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar [2].

(5) Bestämmelserna i detta beslut antas utan att det påverkar artikel 16 i EUF-fördraget och Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter [3].

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

Detta beslut gäller Europaparlamentets framställning, mottagande, överlämnande och lagring av sekretessbelagda uppgifter i syfte att skapa ett lämpligt skydd för dess konfidentiella karaktär. Beslutet genomför framför allt bilaga 2 till ramavtalet.

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

[2] EGT L 145, 31.5.2001, s. 43.

[3] EGT L 8, 12.1.2001, s. 1.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner:

a) *uppgifter/information:* alla muntliga eller skriftliga uppgifter, oavsett överföringsmedium eller upphovsman.

b) *sekretessbelagda uppgifter*: säkerhetsklassificerade sekretessbelagda EU-uppgifter och andra sekretessbelagda uppgifter som inte säkerhetsklassificerats.

c) *sekretessbelagda EU-uppgifter*: alla uppgifter och allt material som klassificerats som TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED vars röjande utan tillstånd skulle kunna vålla unionens eller en eller flera av dess medlemsstaters väsentliga intressen skada i varierande grad, oavsett om upphovet till uppgifterna finns inom de institutioner, organ och byråer som har upprättats genom eller på grundval av fördragen eller om uppgifterna harerhållits från en medlemsstat, ett tredjeland eller en internationell organisation. Sekretessbelagda EU-uppgifter delas upp i följande kategorier:

— TRÈS SECRET UE/EU TOP SECRET: denna sekretessgrad används för uppgifter och material vars röjande utan tillstånd skulle kunna vålla unionens eller en eller flera av dess medlemsstaters väsentliga intressen synnerligen allvarlig skada.

— SECRET UE/EU SECRET: denna sekretessgrad används för uppgifter och material vars röjande utan tillstånd skulle kunna vålla unionen eller en eller flera av dess medlemsstaters väsentliga intressen allvarlig skada.

— CONFIDENTIEL UE/EU CONFIDENTIAL: denna sekretessgrad används för uppgifter och material vars röjande utan tillstånd skulle kunna vålla unionens eller en eller flera av dess medlemsstaters väsentliga intressen skada.

— RESTREINT UE/EU RESTRICTED: denna sekretessgrad används för uppgifter och material vars röjande utan tillstånd skulle kunna vara till nackdel för unionens eller en eller flera av dess medlemsstaters intressen.

d) andra sekretessbelagda uppgifter: alla andra sekretessbelagda uppgifter som inte säkerhetsklassificerats, inklusive uppgifter som omfattas av reglerna om uppgiftsskydd och kravet på yrkessekretess, och som framställts i Europaparlamentet eller överlämnats till Europaparlamentet av andra institutioner, organ och byråer som har upprättats genom eller på grundval av fördragen eller av medlemsstaterna.

e) handling: registrerad information, oavsett fysisk form eller egenskaper.

f) material: handlingar eller varje slag av maskin eller utrustning som tillverkats eller håller på att tillverkas.

g) behov av kännedom i tjänsten: behovet att ta del av sekretessbelagda uppgifter för att kunna utföra sitt officiella uppdrag eller arbete.

h) behörighet: ett beslut (efter utförd säkerhetsprövning) av talmannen, om det gäller Europaparlamentets ledamöter, och av generalsekreteraren, om det gäller Europaparlamentets tjänstemän och parlamentets övriga anställda som arbetar för de politiska grupperna, att bevilja en enskild person tillgång till sekretessbelagda EU-uppgifter upp till en viss nivå, på grundval av ett positivt resultat från en säkerhetsprövning (säkerhetsklarering) som har utförts av en nationell myndighet i enlighet med den nationella lagstiftningen och bestämmelserna i del 2 i bilaga I.

i) inplacering i en lägre sekretessgrad: sekretessgraden sänks.

j) hävande av sekretess: uppgifterna är inte längre hemligstämplade.

k) upphovsman: den som har framställt sekretessbelagda EU-uppgifter eller andra sekretessbelagda uppgifter.

l) säkerhetsmeddelande: de tekniska genomförandeåtgärder som fastställs i bilaga II ([1]).

Artikel 3

Grundläggande principer och miniminormer

1. Europaparlamentets hantering av sekretessbelagda uppgifter ska följa de grundläggande principer och miniminormer som fastställs i bilaga I, del 1.

2. Europaparlamentet ska inrätta ett ledningssystem för informationssäkerhet i enlighet med de grundläggande principerna och miniminormerna.Syftet med detta system ska vara att underlätta det parlamentariska och administrativa arbetet samtidigt som man garanterar skyddet för alla sekretessbelagda uppgifter som hanteras av Europaparlamentet, med full respekt för de regler som upphovsmannen till sådana uppgifter har fastställt i säkerhetsmeddelandet.

Behandlingen av sekretessbelagda uppgifter i Europaparlamentets automatiseradeinformationssystem ska genomföras i enlighet med principen om informationssäkerhet och fastställas i säkerhetsmeddelandet.

([1]) Bilagan ska antas.

3. Europaparlamentets ledamöter får ta del av sekretessbelagda uppgifter upp till och inbegripet sekretessgraden CONFIDENTIEL UE/EU CONFIDENTIAL utan att genomgå säkerhetsprövning. För att få ta del uppgifter som klassificerats som CONFIDENTIEL UE/EU CONFIDENTIAL måste ledamöterna underteckna en försäkran på heder och samvete att de inte kommer att röja uppgifternas innehåll för tredje part. Uppgifter med en högre sekretessgrad än CONFIDENTIEL UE/EU CONFIDENTIAL ska enbart vara tillgängliga för ledamöter som har genomgått en säkerhetsprövning på tillräckligt hög nivå.

4. Europaparlamentets tjänstemän och parlamentets övriga anställda som arbetar för de politiska grupperna får ta del av sekretessbelagda uppgifter om det har konstaterats att de har behov av det i tjänsten, och de får ta del av sekretessbelagda uppgifter med högre sekretessgrad än RESTREINT UE/EU RESTRICTED om de har ett intyg på att de har genomgått en säkerhetsprövning för den aktuella nivån.

Artikel 4

Europaparlamentets framställning och hantering av sekretessbelagda uppgifter

1. Europaparlamentets talman, ordföranden för de berörda parlamentsutskotten och generalsekreteraren och/eller en person som han eller hon skriftligen har gett vederbörlig behörighet får framställa sekretessbelagda uppgifter och/eller klassificera uppgifter i enlighet med säkerhetsmeddelandet.

2. Vid framställning av sekretessbelagda uppgifter ska upphovsmannen tilldela en lämplig sekretessgrad i enlighet med de internationella normer och definitioner som anges i bilaga I. Upphovsmannen ska också som en allmän regel bestämma vilka mottagare som är behöriga att ta del av uppgifterna i förhållande till sekretessgraden. Dessa upplysningar ska ges till enheten för behandling av sekretessbelagd information när handlingen lämnas in till denna enhet.

3. Sekretessbelagda uppgifter som omfattas av yrkessekretess ska hanteras i enlighet med de hanteringsanvisningar som anges i säkerhetsmeddelandet.

Artikel 5

Europaparlamentets mottagande av sekretessbelagda uppgifter

1. Sekretessbelagda uppgifter som Europaparlamentet tar emot ska,

— när det gäller sekretessbelagda EU-uppgifter med sekretessgraden RESTREINT UE/EU RESTRICTED och andra sekretessbelagda uppgifter, lämnas till sekretariatet för den parlamentsinstans eller befattningshavare inom parlamentet som har begärt uppgifterna,

— när det gäller sekretessbelagda EU-uppgifter med sekretessgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, lämnas till enheten för behandling av sekretessbelagda uppgifter.

2. Registreringen, lagringen och spårandet av de sekretessbelagda uppgifterna ska säkerställas av sekretariatet för den parlamentsinstans eller befattningshavare som har mottagit uppgifterna eller av enheten för behandling av sekretessbelagda.

3. När det gäller sekretessbelagda uppgifter med sekretessgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller högre som kommissionen överlämnar enligt ramavtalet, ska de överenskomna arrangemang som avses i bilaga II, punkt 3.2, till ramavtalet (gemensam överenskommelse om mottagare, förfarandet för tillgång till uppgifterna, dvs. säkert läsrum och sammanträde inom stängda dörrar m.m.) och som syftar till att bevara uppgifternas sekretess meddelas till sekretariatet för den berörda parlamentsinstansen eller befattningshavaren eller till enheten för behandling av sekretessbelagda uppgifter när de sekretessbelagda uppgifterna lämnas in.

4. De arrangemang som avses i punkt 3 kan också, på motsvarande sätt, tillämpas på lämnandet av sekretessbelagda uppgifter från andra institutioner, organ och byråer som upprättats genom eller på grundval av fördragen eller av medlemsstaterna.

5. Sekretessbelagda EU-uppgifter som har klassificerats som TRÈS SECRET UE/EU TOP SECRET ska överlämnas till Europaparlamentet i enlighet med ytterligare arrangemang som avtalas mellan den parlamentsinstans eller befattningshavare inom parlamentet som begärt uppgifterna och de EU-institutioner eller medlemsstater som lämnar uppgifterna i fråga. Talmanskonferensen ska tillsätta ett tillsynsutskott. Dess syfte ska vara att säkerställa en skyddsnivå som motsvarar sekretessgraden.

Artikel 6

Europaparlamentets överlämnande av sekretessbelagda EU-uppgifter till tredje part

Europaparlamentet får med upphovsmannens samtycke överlämna sekretessbelagda EU-uppgifter till andra institutioner, organ och byråer som upprättats genom eller på grundval av fördragen eller av medlemsstaterna under förutsättning att dessa, när de sekretessbelagda EU-uppgifterna hanteras, ser till att bestämmelserna i detta beslut följs på sina enheter och i sina lokaler.

Artikel 7

Förvaring av och tillgång till sekretessbelagda uppgifter i säkrade utrymmen (säkra läsrum)

1. Säkra läsrum ska erbjuda utrymme för säker lagring; läsrummen får inte innehålla kopieringsmaskin, telefon, telefax, skanner eller annan teknisk utrustning för reproduktion eller överföring av handlingar.

2. Följande villkor ska gälla för tillträde till ett säkert läsrum.

a) Endast följande personer har tillträde:

— Europaparlamentets ledamöter samt vederbörligen identifierade tjänstemän vid Europaparlamentet och övriga anställda vid parlamentet som arbetar för de politiska grupperna, i enlighet med de arrangemang som avses i artiklarna 4.2 eller 5.3 och 5.4,

— de tjänstemän vid Europaparlamentet som arbetar vid enheten för behandling av sekretessbelagd information,

— när så krävs, de tjänstemän vid Europaparlamentet som ansvarar för säkerhet och brandsäkerhet.

Städning av de säkrade utrymmen får endast ske i närvaro och under noggrann uppsikt av en tjänsteman som arbetar vid enheten för behandling av sekretessbelagd information.

b) Varje person som önskar få tillgång till sekretessbelagda uppgifter ska i förväg lämna sitt namn till enheten för behandling av sekretessbelagd information. Denne ska kontrollera identiteten för varje person som lämnar in en ansökan om att få ta del av dessa uppgifter och i tillämpliga fall kontrollera huruvida denna person har genomgått säkerhetsprövning på den nivå som krävs och är behörig att ta del av uppgifterna i enlighet med de arrangemang som avses i artiklarna 4.2 eller 5.3 och 5.4.

c) Enheten för behandling av sekretessbelagd information har befogenhet att neka varje person som inte är behörig enligt leden a och b tillträde till rummet. Invändningar mot ett beslut från enheten för behandling av sekretessbelagd information ska, när det gäller ledamöter i Europaparlamentet, sändas till talmannen och i övriga fall till generalsekreteraren.

3. Följande villkor ska gälla för tillgång till sekretessbelagda uppgifter i säkerhetsrummet:

a) De personer som har behörighet att ta del av en eller flera handlingar och som har lämnat in en ansökan i enlighet med punkt 2 b ska personligen infinna sig på enheten för behandling av sekretessbelagd information.

Förutom i undantagsfall (t.ex. när många ansökningar om tillgång till uppgifter har framställts under en kort tid) får bara en person åt gången ta del av sekretessbelagd information i säkerhetsrummet i närvaro av en tjänsteman från enheten för behandling av sekretessbelagd information.

Denne tjänsteman ska upplysa den person som är behörig att ta del av den sekretessbelagda informationen om hans/hennes skyldigheter och särskilt se till att personen i fråga undertecknar en försäkran på heder och samvete enligt vilken han/hon förbinder sig att inte röja uppgifternas innehåll för tredje part.

b) När informationen konsulteras får ingen kontakt med omvärlden förekomma (inbegripet via telefon eller annan teknisk utrustning); det är förbjudet att ta anteckningar, och den konsulterade sekretessbelagda informationen får inte kopieras eller fotograferas.

c) Innan en person tillåts lämna det säkra läsrummet ska den ansvarige tjänstemannen från enheten för behandling av sekretessbelagd information försäkra sig om att de konsulterade sekretessbelagda handlingarna är kvar och kontrollera att de är intakta och fullständiga.

4. Om ovanstående regler inte följs ska den ansvarige tjänstemannen från enheten för behandling av sekretessbelagd information informera generalsekreteraren, som ska hänskjuta frågan till talmannen om det är en ledamot i Europaparlamentet som brutit mot reglerna.

Artikel 8

Minimistandarder för övrig konsultation av sekretessbelagda uppgifter

1. När det gäller den administrativa hanteringen av sekretessbelagda handlingar vid ett sammanträde inom stängda dörrar ska sekretariatet för den parlamentsinstans eller den befattningshavare inom parlamentet som ansvarar för sammanträdet se till att följande regler följs:

— Endast de personer som är kallade att delta i sammanträdet och som har genomgått den nödvändiga säkerhetsprövningen får släppas in i sammanträdesrummet.

— Alla handlingar ska vara numrerade, delas ut vid sammanträdets början och samlas in vid dess slut. Handlingarna får inte skrivas av, fotokopieras eller fotograferas.

— Protokollet från sammanträdet ska inte redogöra för innehållet i diskussioner om information som behandlas under sekretess.

— Sekretessbelagda uppgifter som muntligen meddelats mottagare i Europaparlamentet är föremål för samma sekretess som tillämpas på skriftliga sekretessbelagda uppgifter. Detta kan innebära att uppgifternas mottagare måste försäkra på heder och samvete att inte röja uppgifterna för tredje part.

2. Följande regler ska gälla när sekretariatet för parlamentsinstansen eller befattningshavaren inom parlamentet hanterar sekretessbelagda handlingar utanför sammanträdet inom stängda dörrar:

— Pappersutskriften av handlingarna ska överlämnas personligen till chefen för sekretariatet, som ska registrera dem och utfärda ett mottagningsbevis.

— Handlingarna ska förvaras i ett låst utrymme på sekretariatets ansvar när de inte används.

— Utan att det påverkar tillämpningen av punkt 1 för den administrativa hanteringen av sekretessbelagda handlingar vid ett sammanträde inom stängda dörrar, får dessa handlingar under inga omständigheter kopieras, sparas på ett annat medium eller överlämnas till någon person.

— Tillgången till sådana handlingar ska vara begränsad till adressaterna, och ska ske under övervakning av sekretariatet, i enlighet med de arrangemang som avses i artiklarna 4.2 eller 5.3 och 5.4.

— Sekretariatet ska föra ett register över de personer som har tagit del av handlingarna, med uppgift om datum och klockslag för när detta skedde. Denna information ska överlämnas till enheten för behandling av sekretessbelagd information med hänsyn till den årsrapport som ska tas fram enligt artikel 12.

Artikel 9

Arkivering av sekretessbelagda handlingar

1. I Europaparlamentets lokaler ska det finnas ett säkert arkiveringssystem.

Sekretessbelagda handlingar som har lämnats in för slutgiltig förvaring hos enheten för behandling av sekretessbelagd information eller på sekretariatet för parlamentsinstansen/befattningshavaren inom parlamentet ska överföras till säkerhetsarkivet hos enheten för behandling av sekretessbelagd information sex månader efter den senaste konsultationen, dock senast ett år efter att handlingen lämnats in.

2. Enheten för behandling av sekretessbelagd information ska ansvara för förvaltningen av säkerhetsarkivet i enlighet med normal arkiveringsstandard.

3. Följande villkor gäller för konsultation av sekretessbelagda handlingar i säkerhetsarkivet:

— Arkivet får endast konsulteras av de personer vars namn eller tjänst anges i den följehandling som fylls i då den sekretessbelagda handlingen lämnas in.

— En begäran om att få konsultera en sekretessbelagd handling ska lämnas till enheten för behandling av sekretessbelagd information, som ser till att handlingen överförs från arkivet till det säkra läsrummet.

— Vid konsultation gäller de regler och förfaranden som anges i artikel 7 om tillgång till sekretessbelagda uppgifter.

Artikel 10

Inplacering i en lägre sekretessgrad och hävande av sekretess för sekretessbelagda EU-uppgifter

1. Sekretessbelagda EU-uppgifter kan inplaceras i en lägre sekretessgrad eller bli föremål för hävande av sekretess endast efter tillstånd av upphovsmannen och, om så krävs, efter diskussion med andra berörda parter. Inplacering i en lägre sekretessgrad eller hävande av sekretess ska bekräftas skriftligen. Upphovsmannen är ansvarig för att informera sina mottagare om ändringen, och dessa är i sin tur ansvariga för att informera eventuella efterföljande mottagare till vilka de har översänt handlingen eller en kopia av den.Om det är möjligt ska upphovsmannen på den sekretessbelagda handlingen ange ett datum, en tidsperiod eller en händelse när uppgifterna får placeras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall ska upphovsmannen se över handlingarna minst vart femte år för att förvissa sig om att den ursprungliga sekretessklassificeringen fortfarande är nödvändig.

2. Sekretessen för handlingar i säkerhetsarkivet hävs senast efter 30 år, i enlighet med rådets förordning (EEG, Euratom) nr 354/83 av den 1 februari 1983 om öppnandet för allmänheten av Europeiska ekonomiska gemenskapens och Europeiska atomenergigemenskapens historiska arkiv ([1]). Inplacering i en lägre sekretessgrad företas av de sekretessbelagda uppgifternas upphovsman eller den enhet som vid den aktuella tidpunkten är ansvarig enligt bilaga I, del 1, punkt 10.

Artikel 11

Sekretessbrott

1. Brott mot sekretess i allmänhet och mot detta beslut i synnerhet medför, när det gäller ledamöter i Europaparlamentet, tillämpning av de relevanta bestämmelser avseende påföljder som återfinns i Europaparlamentets arbetsordning.

2. Sekretessbrott som begås av anställda medför tillämpning av de förfaranden och påföljder som återfinns i tjänsteföreskrifterna för tjänstemän respektive anställningsvillkoren för övriga anställda i Europeiska unionen, fastställda i förordning (EEG, Euratom, EKSG) nr 259/68 ([2]) (*tjänsteföreskrifterna*).

3. Talmannen och generalsekreteraren ska låta genomföra de eventuella utredningar som krävs.

Artikel 12

Anpassning av detta beslut och av genomförandebestämmelserna samt årlig rapportering om tillämpningen av detta beslut

1. Generalsekreteraren ska föreslå eventuella nödvändiga anpassningar av detta beslut och av genomförandebestämmelserna i bilagorna samt sända dessa förslag till presidiet för beslut.

2. Generalsekreteraren ska sända en årlig rapport till presidiet om tillämpningen av detta beslut.

([1]) EUT L 43, 15.2.1983, s. 1.
([2]) EGT L 56, 4.3.1968, s. 1.

Artikel 13

Övergångsbestämmelser och slutbestämmelser

1. Sekretessbelagda uppgifter som finns hos enheten för behandling av sekretessbelagd information eller i arkiven innan detta beslut blir tillämpligt ska rutinmässigt klassificeras som RESTREINT UE/EU RESTRICTED om inte dess upphovsman antingen beslutar att inte sekretessbelägga handlingen, att ge den en högre sekretessgrad eller att förse den med en märkning inom ett år från det att detta beslut träder i kraft.

2. Om upphovsmannen beslutar att ge sekretessbelagda uppgifter en högre sekretessgrad, ska upphovsmannen eller av denne utsedda personer klassificera de med lägsta möjliga grad, i samråd med enheten för behandling av sekretessbelagd information och i enlighet med kriterierna i bilaga I.

3. Presidiets beslut av den 13 november 2006 om bestämmelserna om förvaltningens hantering av sekretessbelagda handlingar upphävs.

4. Presidiets beslut av den 24 oktober 2005, med mandat för generalsekreteraren att inrätta en kommitté för offentliggörande av handlingar och att anta beslut om offentliggörande av handlingar, upphävs.

Artikel 14

Ikraftträdande

1. Dettabeslut träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

2. Det ska tillämpas från och med den 1 juli 2011.

BILAGA I

DEL 1

GRUNDLÄGGANDE PRINCIPER OCH MINIMINORMER FÖR SÄKERHET NÄR DET GÄLLER SKYDD AV SEKRETESSBELAGDA UPPGIFTER

1. Inledning

I dessa bestämmelser fastställs de grundläggande principer och miniminormer för säkerhet som ska följas av Europaparlamentet på alla dess anställningsorter, samt av alla mottagare av sekretessbelagda EU-uppgifter och annan sekretessbelagd information, så att säkerheten garanteras och berörda personer kan vara förvissade om att det råder en gemensam standard för skyddet. Bestämmelserna åtföljs av regler om hur parlamentsutskotten och andra parlamentsinstanser eller befattningshavare inom parlamentet ska behandla sekretessbelagd information.

2. Allmänna principer

Europaparlamentets säkerhetspolicy utgör en del av dess allmänna interna förvaltningspolicy och grundar sig således på de principer som ligger till grund för denna allmänna policy. Dessa principer innefattar laglighet, öppenhet och insyn, ansvarsskyldighet samt subsidiaritet och proportionalitet.

Laglighetsprincipen innebär behovet att strikt följa de rättsliga ramarna i genomförandet av säkerhetsföreskrifterna och att följa de tillämpliga rättsliga kraven. Det innebär också att ansvaret på säkerhetsområdet måsta grunda sig på vederbörliga rättsliga bestämmelser. Bestämmelserna i tjänsteföreskrifterna, särskilt artikel 17 om personalens skyldighet att inte utan tillstånd lämna ut uppgifter som de fått tillgång till i tjänsten samt avdelning VI om disciplinära åtgärder, gäller till fullo. Slutligen innebär det att sekretessbrott inom Europaparlamentets ansvarsområde måste hanteras på ett sätt som överensstämmer med Europaparlamentets policy för disciplinära åtgärder.

Principen om öppenhet och insyn innebär behovet av tydlighet avseende alla säkerhetsbestämmelser och säkerhetsföreskrifter för att en avvägning ska kunna göras mellan olika tjänster och olika områden (fysisk säkerhet jämfört med informationsskydd osv.) och av en konsekvent och strukturerad policy för säkerhetsmedvetenhet. Det innebär också att tydliga, skriftliga riktlinjer är nödvändiga för genomförande av säkerhetsåtgärder.

Principen om ansvarsskyldighet innebär att ansvarsförhållanden på säkerhetsområdet tydligt definieras. Dessutom innebär det behovet att regelbundet övervaka om dessa ansvarsförhållanden har fullgjorts på korrekt sätt.

Subsidiaritetsprincipen innebär att säkerhet ska organiseras på lägsta möjliga nivå och så nära Europaparlamentets generaldirektorat och enheter som möjligt. Proportionalitetsprincipen innebär att säkerhetsverksamheten strikt ska begränsas till vad som är absolut nödvändigt och att säkerhetsåtgärderna ska stå i proportion till de intressen som ska skyddas samt till det faktiska och potentiella hotet mot dessa intressen, så att de kan skyddas på ett sätt som orsakar minsta möjliga störning.

3. Grunderna för informationssäkerhet

Grunderna för en god informationssäkerhet är följande:

a) I Europaparlamentet: en teknisk enhett för informationssäkerhet (Infosec) som är ansvarig för att tillsammans med den berörda säkerhetsmyndigheten tillhandahålla information och ge råd om tekniska hot mot säkerheten och vilka skyddsåtgärder som kan vidtas.

b) Ett nära samarbete mellan Europaparlamentets ansvariga enheter och övriga EU-institutioners säkerhetstjänster.

4. Principer för informationssäkerhet

4.1 *Mål*

Informationssäkerhetens huvudsyften är:

a) att skydda sekretessbelagda EU-uppgifter och annan sekretessbelagd information mot spioneri, sekretessbrott och obehörigt röjande,

b) att skydda sekretessbelagda EU-uppgifter som hanteras i nätverk och system för kommunikation och information mot hot som riktar sig mot uppgifternas sekretess, integritet och tillgänglighet,

c) att skydda Europaparlamentets lokaler där sekretessbelagda EU-uppgifter förvaras från sabotage och uppsåtlig skadegörelse,

d) i händelse av en säkerhetsbrist, att bedöma omfattningen av den skada som åsamkats, begränsa följderna av den, genomföra säkerhetsutredningar och vidta nödvändiga avhjälpande åtgärder.

4.2 *Sekretessbeläggning*

4.2.1 I sekretessfrågor krävs det omsorg och erfarenhet vid valet av vilka uppgifter och vilket material som ska skyddas och bedömningen av vilken skyddsnivå som krävs. Grundläggande är att skyddsnivån ska motsvara känsligheten hos de enskilda uppgifterna eller det material som ska skyddas. För att säkerställa ett smidigt informationsflöde ska såväl överdriven sekretessbeläggning som fall där sekretessbeläggningen inte är tillräcklig undvikas.

4.2.2 Systemet för sekretessbeläggning är det instrument som ska användas för att omsätta principerna som fastställs i detta avsnitt i praktiken. Ett liknande system för sekretessbeläggning ska följas i planeringen och organiseringen av arbetet mot spionerі, sabotage, terrorism och andra hot, så att de viktigaste utrymmen där sekretessbelagda EU-uppgifter förvaras och de känsligaste punkterna i dessa får högsta möjliga skyddsnivå.

4.2.3 Ansvaret för sekretessbeläggning ligger enbart hos uppgifternas upphovsman.

4.2.4 Sekretessgraden ska endast grunda sig på uppgifternas innehåll.

4.2.5 Sekretessgraden för ett antal uppgifter i grupp ska som helhet vara minst densamma som den del som fått den högsta sekretessgraden. Samlade uppgifter får dock ges en högre sekretessgrad än de enskilda uppgifter som ingår.

4.2.6 Uppgifter ska endast sekretessbeläggas när det är nödvändigt och under så lång tid som är nödvändigt.

4.3 *Syftet med säkerhetsåtgärderna*

Säkerhetsåtgärderna ska:

a) omfatta alla personer som har tillgång till sekretessbelagda EU-uppgifter, sekretessbelagda EU-uppgiftsbärande medier och annan sekretessbelagd information samt utrymmen där sådana uppgifter förvaras och viktiga anläggningar finns,

b) vara utformade så att personer upptäcks vars ställning kan äventyra säkerheten för sådana uppgifter och för viktiga anläggningar där sådana uppgifter förvaras, och kunna utestänga eller avlägsna dessa personer,

c) hindra obehöriga från att få tillgång till sådana uppgifter eller de anläggningar där uppgifterna förvaras,

d) säkerställa att sådana uppgifter sprids endast på grundval av principen om behov av kännedom i tjänsten, som är grundläggande för alla aspekter av säkerhet,

e) säkerställa integriteten för (dvs. förebygga förvanskning, obehörig ändring eller radering) och tillgängligheten (dvs. för de som behöver och är behöriga att få tillgång till uppgifterna) till alla sekretessbelagda uppgifter , oavsett om de är säkerhetsklassificerade eller inte, särskilt för sådana uppgifter som lagras, bearbetas eller överförs i elektronisk form.

5. **Gemensamma miniminormer**

Europaparlamentet ska se till att gemensamma miniminormer för säkerhet följs av alla mottagare av sekretessbelagda EU-uppgifter, både inom institutionen och under dess befogenhet, inbegripet alla dess enheter och uppdragstagare, så att sådana uppgifter kan föras vidare i förvissning om att de kommer att hanteras med samma omsorg överallt. Sådana miniminormer ska omfatta kriterier för säkerhetsprövning av Europaparlamentets tjänstemän och övriga anställda vid parlamentet som arbetar för de politiska grupperna samt förfaranden för skydd av sekretessbelagda uppgifter.

Europaparlamentet får tillåta att sådana uppgifter vidarebefordras till utomstående instanser bara om dessa kan garantera att de följer föreskrifter som minst motsvarar dessa gemensamma miniminormerna när de hanterar uppgifterna.

Sådana gemensamma miniminormer ska också tillämpas när Europaparlamentet enligt kontrakt eller bidragsöverenskommelser, tilldelar uppgifter till företag eller andra enheter vilka medför sekretessbelagda uppgifter.

6. **Säkerheten för Europaparlamentets tjänstemän och övriga anställda vid parlamentet som arbetar för de politiska grupperna**

6.1 *Säkerhetsanvisningar för Europaparlamentets tjänstemän och övriga anställda vid parlamentet som arbetar för de politiska grupperna*

Europaparlamentets tjänstemän och övriga anställda vid parlamentet som arbetar för de politiska grupperna, vilkas tjänster innebär att de kan få tillgång till sekretessbelagda EU-uppgifter, ska både när de börjar sin tjänst och därefter med jämna mellanrum ges noggranna instruktioner om kraven på säkerhet och hur denna säkerhet erhålls. Dessa personer ska skriftligen intyga att de till fullo har läst och förstått dessa säkerhetsbestämmelser.

6.2 *Ledningsansvar*

Arbetsledningen ska ha skyldighet att känna till vilka i personalen som arbetar med sekretessbelagda uppgifter eller som har tillgång till skyddade kommunikations- eller informationssystem samt registrera och rapportera incidenter eller uppenbara sårbarheter som skulle kunna påverka säkerheten.

6.3 *Säkerhetsstatusen för Europaparlamentets tjänstemän och övriga anställda vid parlamentet som arbetar för de politiska grupperna*

Förfaranden ska fastställas för att säkerställa att det, när negativa uppgifter kommer fram om en av Europaparlamentets tjänstemän eller övriga anställda vid parlamentet som arbetar för en politisk grupp, vidtas åtgärder för att fastställa huruvida denna persons arbete innebär kontakt med sekretessbelagda uppgifter eller huruvida vederbörande har tillgång till skyddade kommunikations- eller informationssystem, och att Europaparlamentets ansvariga enhet informeras. Om det fastställs att personen utgör en säkerhetsrisk ska han eller hon avstängas eller avlägsnas från sådana uppdrag där han eller hon skulle kunna äventyra säkerheten.

7. **Fysisk säkerhet**

Fysisk säkerhet innebär tillämpning av fysiska och tekniska skyddsåtgärder för att hindra obehörigt tillträde till sekretessbelagda EU-uppgifter.

7.1 *Behov av skydd*

Den grad av fysiska säkerhetsåtgärder som ska tillämpas för att skydda sekretessbelagda EU-uppgifter ska stå i proportion till sekretessgraden för och omfattningen av och hotet mot uppgifterna och materialet. Alla som har tillgång till sekretessbelagda EU-uppgifter ska tillämpa enhetliga rutiner för sekretessbeläggning av dessa uppgifter och ska följa gemensamma skyddsnormer för hur uppgifter och material som kräver skydd ska förvaras, överföras och förstöras.

7.2 *Kontroll*

Innan personer som har ansvar för sekretessbelagda EU-uppgifter lämnar obevakade utrymmen ska de se till att uppgifterna är i säkert förvar och att alla säkerhetsanordningar har aktiverats (lås, larm osv.). Ytterligare oberoende kontroller ska utföras efter kontorstid.

7.3 *Byggnadernas säkerhet*

Byggnader där sekretessbelagda EU-uppgifter förvaras eller där det finns skyddade kommunikations- eller informationssystem ska skyddas mot obehörigt tillträde.

Arten av skydd för sekretessbelagda EU-uppgifter, t.ex. galler för fönster, lås för dörrar, vakter vid ingångarna, automatiska system för kontroll av tillträde, säkerhetskontroller och patruller, larmsystem, system för upptäckt av intrång och vakthundar, ska vara avhängig:

a) sekretessgraden för och omfattningen av de uppgifter och det material som ska skyddas samt var i byggnaden detta förvaras,

b) kvaliteten på säkerhetsskåpen för uppgifterna och materialet i fråga, och

c) byggnadens konstruktion och belägenhet.

Arten av skydd för kommunikations- eller informationssystem ska vara avhängig av vilken bedömning som gjorts av värdet på de tillgångar som står på spel och av den potentiella skadan vid sekretessbrott, hur den byggnad där systemet finns är konstruerad samt dess belägenhet och var i byggnaden systemet finns.

7.4 *Beredskapsplaner*

Detaljerade planer ska utarbetas i förväg för hur sekretessbelagda uppgifter ska skyddas i händelse av en nödsituation.

8. **Säkerhetsbeteckningar, markeringar, fastsättande och hantering av sekretessgrader**

8.1 *Säkerhetsbeteckningar*

Inga andra sekretessgrader än dem som definieras i artikel 2 c i detta beslut är tillåtna.

För att begränsa en sekretessgrads giltighet (för sekretessbelagda uppgifter som innebär en automatisk inplacering i en lägre sekretessgrad eller hävande av sekretess) får en överenskommen säkerhetsbeteckning användas. Denna beteckning ska antingen vara ”UNTIL (till och med) … (tidpunkt/datum)” eller ”UNTIL (fram till) … (händelse)”.

Tilläggsmarkeringar, t.ex. CRYPTO eller någon annan säkerhetsbeteckning som är erkänd inom EU, ska användas när det är nödvändigt att begränsa utlämnandet och det krävs särskild hantering utöver vad som framgår av sekretessgraden.

Säkerhetsbeteckningar ska endast användas tillsammans med en sekretessgrad.

8.2 *Markeringar*

En markering får användas för att ange vilket område en viss handling omfattar eller särskild spridning, grundad på behovet att få tillgång till uppgifterna för tjänsteutövningen, eller (för icke-sekretessbelagda uppgifter) för att markera slutet på ett handelsförbud.

En markering är inte en sekretessgrad och får inte användas i stället för en sådan.

8.3 *Fastsättande av sekretessgrader och säkerhetsbeteckningar*

Sekretessgrader ska fastsättas enligt följande:

a) Handlingar med beteckningen RESTREINT UE/EU RESTRICTED: på mekanisk eller elektronisk väg.

b) Handlingar med beteckningen CONFIDENTIEL UE/EU CONFIDENTIAL: på mekanisk väg, för hand eller genom tryck på förstämplat, registrerat papper.

c) Handlingar med beteckningen SECRET UE/EU SECRET och TRÈS SECRET UE/EU TOP SECRET, på mekanisk väg eller för hand.

Säkerhetsbeteckningar ska sättas fast omedelbart under sekretessgraden och med samma metod som använts för denna.

8.4 *Hantering av sekretessgrader*

8.4.1 Allmänt

Uppgifter ska sekretessbeläggas bara när det är nödvändigt. Sekretessgraden ska anges tydligt och korrekt, och ska upprätthållas bara så länge som uppgifterna kräver skydd.

Ansvaret för att sekretessbelägga uppgifter och för en eventuell senare inplacering i en lägre sekretessgrad eller för hävande av sekretessen vilar helt på upphovsmannen.

Europaparlamentets tjänstemän ska sekretessbelägga, inplacera i en lägre sekretessgrad eller häva sekretessen på uppdrag av eller genom delegering från generalsekreteraren.

De detaljerade förfarandena för hantering av sekretessbelagda handlingar ska vara utformade så att de säkerställer att dessa får ett lämpligt skydd med hänsyn till de uppgifter de innehåller.

De personer som har behörighet att bli upphovsmän till handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET ska vara så få som möjligt, och deras namn ska finnas på en förteckning som upprättas av enheten för behandling av sekretessbelagd information.

8.4.2 Tillämpning av sekretessbeläggning

Sekretessgraden för en handling ska fastställas med utgångspunkt i hur känsligt handlingens innehåll är, i enlighet med definitionerna i artikel 2. Det är viktigt att sekretessbeläggningen utförs korrekt och används sparsamt, särskilt när det gäller sekretessgraden TRÈS SECRET UE/EU TOP SECRET.

Sekretessgraden för en skrivelse eller en not som åtföljs av bilagor ska vara densamma som den högsta sekretessgraden som beviljats en av bilagorna. Upphovsmannen ska tydligt ange med vilken sekretessgrad skrivelsen eller noten ska förses när den skilts från de bifogade handlingarna.

Upphovsmannen till en handling som ska sekretessbeläggas ska ha ovanstående bestämmelser i åtanke och ska hejda alla tendenser till för hög eller för låg sekretessgrad.

Enstaka sidor, stycken, avsnitt, bilagor, tillägg och bifogade ark till en viss handling kan kräva inplacering i en annan sekretessgrad och ska sekretessbeläggas i enlighet med detta. Sekretessgraden för handlingen som helhet ska vara densamma som den del som fått den högsta sekretessgraden.

9. **Inspektioner**

Periodiska inspektioner av säkerhetsarrangemangen för skydd av sekretessbelagda EU-uppgifter ska utföras av Europaparlamentets direktorat som ansvarar för säkerhet, eventuellt med stöd av enheten för behandling av sekretessbelagd information.

Europaparlamentets direktorat som ansvarar för säkerhet och säkerhetstjänster från andra institutioner, organ och byråer som har upprättats genom eller på grundval av fördragen som innehar sekretessbelagda EU-uppgifter får också komma överens om att genomföra utvärderingar korsvis av varandras säkerhetsarrangemang för skydd av sekretessbelagda EU-uppgifter.

10. **Förfarande för hävande av sekretess**

10.1 Enheten för behandling av sekretessbelagd information ska granska sekretessbelagda EU-uppgifter och lämna förslag på hävande av sekretessen till upphovsmannen av handlingen allra senast 25 år efter dagen för dess upprättande. Handlingar för vilka sekretessen inte hävts vid den första granskningen ska regelbundet, dock minst vart femte år, granskas på nytt.

10.2 Förutom på handlingar som fysiskt befinner sig i säkerhetsarkivet och som sekretessbelagts får förfarandet för hävande av sekretess också tillämpas på andra sekretessbelagda uppgifter som finns i säkerhetsarkivet eller i Europaparlamentets Centrum för arkiv och dokumentation (Cardoc).

10.3 Enheten för behandling av sekretessbelagd information ska i upphovsmannens ställe ha ansvaret för att informera handlingens mottagare om förändringen av sekretessgraden, och dessa mottagare ska i sin tur vara ansvariga för att informera eventuella efterföljande mottagare till vilka de har översänt handlingen eller en kopia av den om ändringen.

10.4 Ett hävande av sekretessen ska inte påverka eventuella markeringar som kan finnas i handlingen.

10.5 Den ursprungliga sekretessgraden, som är angiven upptill och nedtill på varje sida, ska strykas över. Första sidan (försättsbladet) i handlingen ska stämplas och förses med en referensuppgift från enheten för behandling av sekretessbelagd information.

10.6 Texten till handlingen för vilken sekretessen hävts ska bifogas det elektroniska registerkortet eller det motsvarande system där handlingen är registrerad.

10.7 När det gäller känsliga handlingar och handlingar som omfattas av undantagen som rör den enskildes privatliv och personliga integritet eller en fysisk eller juridisk persons affärsintressen ska artikel 2 i förordning (EEG, Euratom) nr 354/83 vara tillämplig.

10.8 Utöver bestämmelserna i 10.1 till 10.7 ska följande regler gälla:

a) När det gäller handlingar från tredje part ska enheten för behandling av sekretessbelagd information samråda med denna tredje part innan sekretessen hävs. Den tredje parten har åtta veckor på sig att inkomma med synpunkter.

b) När det gäller undantaget som rör den enskildes privatliv och personliga integritet ska förfarandet för att häva sekretessen särskilt beakta om den berörda personen samtycker, om det är omöjligt att fastställa identiteten för den berörda personen och/eller om personen i fråga är avliden.

c) När det gäller undantaget som rör en fysisk eller juridisk persons affärsintressen kan den berörda personen underrättas via offentliggörande i *Europeiska unionens officiella tidning* och ges en tidsfrist på fyra veckor från dagen för offentliggörandet att lämna in eventuella synpunkter.

DEL 2

FÖRFARANDE FÖR SÄKERHETSPRÖVNING

11. Förfarande för säkerhetsprövning av europaparlamentets ledamöter

11.1 Mot bakgrund av Europaparlamentets rättigheter och befogenheter får dess ledamöter ges tillgång till sekretessbelagda EU-uppgifter upp till och med sekretessgraden CONFIDENTIEL UE/EU CONFIDENTIAL utan säkerhetsprövning. För att få ta del av uppgifter med beteckningen CONFIDENTIEL UE/EU CONFIDENTIAL måste ledamöterna underteckna en försäkran på heder och samvete att de inte kommer att röja uppgifterna för tredje part.

11.2 För att få tillgång till uppgifter med beteckningarna TRÈS SECRET UE/EU TOP SECRET och SECRET UE/EU SECRET måste ledamöterna ha getts behörighet i enlighet med det förfarande som avses i punkterna 11.3 och 11.4.

11.3 Behörighet ska endast beviljas Europaparlamentets ledamöter som har genomgått en säkerhetsprövning av de behöriga nationella myndigheterna i medlemsstaterna i enlighet med förfarandet i punkterna11.9–11.14. Talmannen ska vara ansvarig för att bevilja ledamöterna behörighet.

11.4 Talmannen får bevilja behörighet efter att ha inhämtat ett yttrande från de behöriga nationella myndigheterna i medlemsstaterna på grundval av den säkerhetsprövning som genomförts i enlighet med punkterna 11.8–11.13.

11.5 Europaparlamentets direktorat som ansvarar för säkerhet ska föra en aktuell förteckning över alla Europaparlamentets ledamöter som beviljats behörighet, inklusive tillfällig behörighet som avses i punkt 11.15.

11.6 Behörigheten ska vara giltig för en period av fem år eller för den tid som uppgifterna, som låg till grund för att den beviljades, varar. Den får förnyas i enlighet med förfarandet som fastställs i punkt 11.4.

11.7 Behörigheten ska dras in av talmannen om han eller hon anser att det är motiverat. Ett beslut om indragen behörighet ska meddelas dels den berörda ledamoten i Europaparlamentet, som kan begära att höras av talmannen innan indragandet träder i kraft, dels den behöriga nationella myndigheten.

11.8 Säkerhetsprövningen ska genomföras med bistånd av den berörda ledamoten i Europaparlamentet och på begäran av talmannen. Den behöriga nationella myndigheten för prövning ska vara den i den medlemsstat där den aktuella ledamoten är medborgare.

11.9 Som en del av prövningsförfarandet ska den berörda ledamoten i Europaparlamentet fylla i ett formulär med personliga uppgifter.

11.10 Talmannen ska i sin begäran till de behöriga nationella myndigheterna ange nivån på de sekretessbelagda uppgifter som den berörda ledamoten i Europaparlamentet ska få tillgång till, så att de kan genomföra säkerhetsprövningen.

11.11 Hela säkerhetsprövningsprocessen, som den genomförs av de behöriga nationella myndigheterna, ska tillsammans med de erhållna resultaten stå i överensstämmelse med de relevanta regler och förordningar som gäller i den berörda medlemsstaten, inklusive sådana som rör överklagande.

11.12 Om medlemsstatens behöriga nationella myndigheter avger ett positivt yttrande får talmannen bevilja den berörda ledamoten i Europaparlamentet behörighet.

11.13 Ett negativt yttrande från de behöriga nationella myndigheterna ska meddelas den berörda ledamoten i Europaparlamentet, som kan begära att höras av talmannen. Om talmannen anser det nödvändigt får han eller hon begära ytterligare förtydliganden från de behöriga nationella myndigheterna. Om det negativa yttrandet kvarstår ska behörighet inte beviljas.

11.14 Alla ledamöter i Europaparlamentet som beviljats behörighet enligt punkt 11.3 ska, när behörigheten beviljas och därefter med jämna mellanrum, erhålla alla nödvändiga anvisningar angående skyddet av sekretessbelagda uppgifter och hur detta skydd ska säkerställas. Ledamöterna ska underteckna en förklaring om att de mottagit dessa anvisningar.

11.15 Talmannen får i undantagsfall, efter att i förväg ha informerat de behöriga nationella myndigheterna och förutsatt att de inte har hört av sig inom en månad, bevilja tillfällig behörighet för en ledamot i Europaparlamentet för en period av högst sex månader, i avvaktan på resultatet av den prövning som avses i punkt 11.11. Den tillfälliga behörighet som beviljas på detta sätt ska inte ge tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET.

12. **Förfarande för säkerhetsprövning av Europaparlamentets tjänstemän och parlamentetes övriga anställda som arbetar för de politiska grupperna**

12.1 Endast Europaparlamentets tjänstemän, och parlamentets övriga anställda som arbetar för de politiska grupperna, som på grund av sina åligganden och för sin tjänsteutövning behöver känna till eller använda sekretessbelagda uppgifter, får ha tillgång till sådana uppgifter.

12.2 För att få tillgång till uppgifter med beteckningarna TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET och CONFIDENTIEL UE/EU CONFIDENTIAL måste de personer som avses i punkt 12.1 ha getts behörighet i enlighet med det förfarande som fastställts i punkterna 12.3 och 12.4.

12.3 Behörighet ska endast beviljas de personer som avses i punkt 12.1 som har genomgått en säkerhetsprövning av de behöriga nationella myndigheterna i medlemsstaterna i enlighet med förfarandet i punkterna 12.9–12.14. Generalsekreteraren ska vara ansvarig för att bevilja behörighet åt Europaparlamentets tjänstemän och parlamentets övriga anställda som arbetar för de politiska grupperna.

12.4 Generalsekreteraren får bevilja behörighet efter att ha inhämtat ett yttrande från de behöriga nationella myndigheterna i medlemsstaterna på grundval av den säkerhetsprövning som genomförts i enlighet med punkterna 12.8–12.13.

12.5 Europaparlamentets direktorat som ansvarar för säkerhet ska föra en aktuell förteckning över alla tjänster som kräver säkerhetsprövning, enligt uppgifter från relevanta avdelningar vid Europaparlamentet, och över alla personer som beviljats behörighet, inklusive tillfällig behörighet enligt punkt 12.15.

12.6 Behörigheten, som ska vara giltig för en period av fem år eller för den tid som uppgifterna, som låg till grund för att den beviljades, varar. Den får förnyas i enlighet med förfarandet i punkt 12.4.

12.7 Behörigheten ska dras in av generalsekreteraren om han eller hon anser att det är motiverat. Ett beslut om indragen behörighet ska meddelas dels den berörda tjänstemannen vid Europaparlamentet eller den anställde vid Europaparlamentet som arbetar för en politisk grupp, som kan begära att höras av generalsekreteraren innan indragandet träder i kraft, dels den behöriga nationella myndigheten.

12.8 Säkerhetsprövningen ska genomföras med bistånd av den berörda personen och på begäran av generalsekreteraren. Den behöriga nationella myndigheten för prövning ska vara den i den medlemsstat där den aktuella personen är medborgare. Om nationella lagar och förordningar så tillåter får de behöriga nationella myndigheter genomföra undersökningar i fråga om icke-medborgare som begär tillgång till uppgifter med sekretessgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

12.9 Som en del av prövningsförfarandet ska den berörda tjänstemannen vid Europaparlamentet eller den anställde vid Europaparlamentet som arbetar för en politisk grupp fylla i ett formulär med personliga uppgifter.

12.10 Generalsekreteraren ska i sin begäran till de behöriga nationella myndigheterna ange nivån på de sekretessbelagda uppgifter som den berörda personen ska få tillgång till, så att de kan genomföra säkerhetsprövningen och yttra sig om på vilken nivå det är lämpligt att bevilja den berörda personen behörighet.

12.11 Hela säkerhetsprövningsprocessen, som den genomförs av de behöriga nationella myndigheterna, ska tillsammans med de erhållna resultaten stå i överensstämmelse med de relevanta regler och förordningar som gäller i den berörda medlemsstaten, inklusive sådana som rör överklagande.

12.12 Om medlemsstatens behöriga nationella myndigheter avger ett positivt yttrande får generalsekreteraren bevilja den berörda personen behörighet.

12.13 Ett negativt yttrande från de behöriga nationella myndigheterna ska meddelas den berörda tjänstemannen vid Europaparlamentet eller den anställde vid parlamentet som arbetar för en politisk grupp, som kan begära att höras av generalsekreteraren. Om generalsekreteraren anser det nödvändigt får han eller hon begära ytterligare förtydliganden från de behöriga nationella myndigheterna. Om det negativa yttrandet kvarstår ska behörighet inte beviljas.

12.14 Alla tjänstemän vid Europaparlamentet och övriga anställda vid parlamentet som arbetar för de politiska grupperna som beviljats behörighet enligt punkt 12.4 och 12.5 ska, när behörigheten beviljas och därefter med jämna mellanrum, erhålla alla nödvändiga anvisningar angående skyddet av sekretessbelagda uppgifter och hur detta skydd ska säkerställas. Dessa tjänstemän och anställda ska underteckna en förklaring om att de mottagit dessa anvisningar och att de åtar sig att följa dem.

12.15 Generalsekreteraren får i undantagsfall, efter att i förväg ha informerat de behöriga nationella myndigheterna och förutsatt att de inte har hört av sig inom en månad, bevilja en tjänsteman vid Europaparlamentet eller en anställd vid parlamentet som arbetar för en politisk grupp tillfällig behörighet för en period av högst sex månader, i avvaktan på resultatet av den prövning som avses i punkt 12.11 i detta avsnitt. Tillfälliga behörigheter som beviljas på detta sätt ska inte ge tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET.