II

(Meddelanden)

MEDDELANDEN FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER OCH ORGAN

EUROPAPARLAMENTET

BESLUT AV EUROPAPARLAMENTETS PRESIDIUM

av den 15 april 2013

om bestämmelserna för Europaparlamentets hantering av sekretessbelagd information

(2014/C 96/01)

EUROPAPARLAMENTETS PRESIDIUM HAR FATTAT DETTA BESLUT

med beaktande av artikel 23.12 i Europaparlamentets arbetsordning,

och av följande skäl:

(1) Mot bakgrund av ramavtalet om förbindelserna mellan Europaparlamentet och Europeiska kommissionen [1] undertecknat den 20 oktober 2010 (*ramavtalet*) och det interinstitutionella avtalet mellan Europaparlamentet och rådet om överförande till och hantering inom Europaparlamentet av säkerhetsskyddsklassificerade uppgifter som innehas av rådet vilka rör andra frågor än de som omfattas av den gemensamma utrikes- och säkerhetspolitiken [2] (*det interinstitutionella avtalet*) undertecknat den 12 mars 2014, är det nödvändigt att fastställa särskilda bestämmelser om Europaparlamentets hantering av sekretessbelagda uppgifter.

(2) Lissabonfördraget ger Europaparlamentet nya uppgifter, och för att utveckla parlamentets verksamhet på de områden som kräver en viss sekretess är det nödvändigt att fastställa grundläggande principer, miniminormer för säkerhet och lämpliga förfaranden för Europaparlamentets hantering av sekretessbelagda uppgifter, inklusive säkerhetsskyddsklassificerade 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 nuvarande och framtida bestämmelser om tillgång till handlingar antagna i enlighet med artikel 15 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

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

(5) Bestämmelserna i detta beslut antas utan att det påverkar nuvarande och framtida bestämmelser om skydd av personuppgifter antagna i enlighet med artikel 16 i EUF-fördraget.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte

Detta beslut reglerar Europaparlamentets förvaltning och hantering av sekretessbelagda uppgifter, inklusive framställning, mottagande, överlämnande och lagring av sådana uppgifter, i syfte att skapa ett lämpligt skydd för deras konfidentiella karaktär. Beslutet genomför framför allt det interinstitutionella avtalet och ramavtalet, särskilt bilaga 2 till det avtalet.

Artikel 2

Definitioner

I detta beslut gäller följande definitioner:

a) *Uppgifter/information*: alla muntliga eller skriftliga uppgifter eller information, oberoende av överföringsmedium eller upphovsman.

b) *Sekretessbelagda uppgifter*: säkerhetsskyddsklassificerade uppgifter och andra sekretessbelagda uppgifter som inte säkerhetsskyddsklassificerats.

c) *Säkerhetsskyddsklassificerade uppgifter:* säkerhetsskyddsklassificerade EU-uppgifter och uppgifter med motsvarande säkerhetsskyddsklassificering.

d) *Säkerhetsskyddsklassificerade EU-uppgifter (EUCI)*: alla uppgifter och allt material som placerats på säkerhetsskyddsklassificeringsnivåerna 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 intressen skada i varierande grad, och upphovet till uppgifterna finns inom de institutioner, organ eller byråer som har upprättats genom eller på grundval av fördragen. Uppgifterna delas upp i följande kategorier:

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

— CONFIDENTIEL UE/EU CONFIDENTIAL är 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 uppgifter och material vars röjande utan tillstånd skulle kunna vara till nackdel för unionens eller en eller flera av dess medlemsstaters intressen.

e) *Uppgifter med motsvarande säkerhetsskyddsklassificering*: säkerhetsskyddsklassificerade uppgifter utfärdade av medlemsstater, tredjeländer eller internationella organisationer, som bär en säkerhetsskyddsklassificeringsmarkering motsvarande en av de säkerhetsskyddsmarkeringar som används för EUCI och som har vidarebefordrats till Europaparlamentet av rådet eller kommissionen.

f) *Andra sekretessbelagda uppgifter*: alla andra sekretessbelagda uppgifter som inte är säkerhetsskyddsklassificerade, inklusive uppgifter som omfattas av reglerna om uppgiftsskydd och kravet på tystnadsplikt, 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.

g) *Handling*: registrerade uppgifter, oberoende av fysisk form eller egenskaper.

h) *Material*: alla slags handlingar eller maskiner eller utrustning som tillverkats eller håller på att tillverkas.

i) *Behov av kännedom i tjänsten*: en persons behov av att ta del av sekretessbelagda uppgifter för att kunna utföra sitt officiella uppdrag eller arbete.

j) *Behörighet*: ett beslut av talmannen, om det gäller Europaparlamentets ledamöter, eller av generalsekreteraren, om det gäller Europaparlamentets tjänstemän och Europaparlamentets övriga anställda som arbetar för de politiska grupperna, att bevilja en enskild person tillgång till säkerhetsskyddsklassificerade uppgifter upp till en viss nivå, på grundval av ett positivt resultat vid en säkerhetsprövning (säkerhetsklarering) som utförts av en nationell säkerhetsmyndighet i enlighet med den nationella lagstiftningen och med bestämmelserna i del 2 i bilaga I.

k) *Placering på en lägre säkerhetsskyddsklassificeringsnivå:* sänkning av säkerhetsskyddsklassificeringsnivån.

l) *Beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade*: borttagande av all säkerhetsskyddsklassificering.

m) *Säkerhetsskyddsmarkering:* en markering som görs på ”andra sekretessbelagda uppgifter” för att visa hur uppgifterna ska hanteras enligt förhandsbestämda specifika anvisningar eller visa vilket område en viss handling omfattar. Markeringen kan även göras på säkerhetsskyddsklassificerade uppgifter för att ställa ytterligare krav på deras hantering.

n) *Avmarkering:* borttagande av alla säkerhetsskyddsmarkeringar.

o) *Upphovsman*: den vederbörligen behöriga person som har framställt sekretessbelagda uppgifter.

p) *Säkerhetsmeddelanden*: de genomförandeåtgärder som fastställs i bilaga II.

q) *Hanteringsanvisningar:* tekniska anvisningar till avdelningarna inom Europaparlamentet om hanteringen av sekretessbelagda uppgifter.

Artikel 3

Grundläggande principer och miniminormer

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

2. Europaparlamentet ska inrätta ett ledningssystem för informationssäkerhet (ledningssystemet) i enlighet med de grundläggande principerna och miniminormerna. Ledningssystemet ska bestå av säkerhetsmeddelanden, hanteringsanvisningar och arbetsordningen. Syftet med ledningssystemet ska vara att underlätta det parlamentariska och administrativa arbetet samtidigt som skyddet för alla sekretessbelagda uppgifter som hanteras av Europaparlamentet säkerställs, med full respekt för de regler som upphovsmannen till sådana uppgifter har fastställt i säkerhetsmeddelandet.

Behandlingen av sekretessbelagda uppgifter i Europaparlamentets automatiserade kommunikations- och informationssystem ska genomföras i enlighet med principen om informationssäkring enligt säkerhetsmeddelande 3.

3. Europaparlamentets ledamöter får ta del av säkerhetsskyddsklassificerade uppgifter upp till och med klassificeringsnivån RESTREINT UE/EU RESTRICTED utan att genomgå någon säkerhetsprövning.

4. För uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande ska tillgång beviljas Europaparlamentets ledamöter som har förklarats behöriga av talmannen enligt artikel 5 eller sedan de undertecknat en försäkran på heder och samvete att de inte kommer att röja uppgifternas innehåll för tredje part och att de iakttar skyldigheten att skydda uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och är medvetna om konsekvenserna av bristande efterlevnad av denna skyldighet.

5. Om de berörda uppgifterna placerats på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller TRÈS SECRET/EU TOP SECRET eller motsvarande ska tillgång beviljas ledamöter av Europaparlamentet som talmannen förklarat som behöriga sedan

a) ledamöterna har genomgått en säkerhetsprövning i enlighet med del 2 i bilaga I i detta beslut, eller

b) ett meddelande har mottagits från en behörig nationell myndighet om att de berörda ledamöterna i kraft av sina arbetsuppgifter är vederbörligen behöriga i enlighet med nationell lagstiftning.

6. Innan Europaparlamentets ledamöter beviljas tillgång till säkerhetsskyddsklassificerade uppgifter ska de informeras om och erkänna sitt ansvar avseende skydd av sådana uppgifter i överensstämmelse med bilaga I. De ska också informeras om medlen för att säkerställa ett sådant skydd.

7. 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 säkerhetsskyddsklassificerade uppgifter som placerats på en högre skyddsnivå än RESTREINT UE/EU RESTRICTED om de har genomgått en säkerhetsprövning för den aktuella nivån. Dessa personer ska beviljas tillgång till säkerhetsskyddsklassificerade uppgifter endast om de har informerats och fått skriftliga anvisningar om sitt ansvar avseende skydd av sådana uppgifter och om medlen för att säkerställa ett sådant skydd, och om de har undertecknat en försäkran där de intygar att de mottagit anvisningarna och förbinder sig att följa dem i överensstämmelse med nuvarande regler.

Artikel 4

Europaparlamentets framställande och hantering av sekretessbelagda uppgifter

1. Europaparlamentets talman, ordförandena för de berörda parlamentsutskotten samt generalsekreteraren och/eller en person som han eller hon skriftligen har gett vederbörlig behörighet, får framställa sekretessbelagda uppgifter och/eller säkerhetsskyddsklassificera uppgifter enligt säkerhetsmeddelandena.

2. Vid framställande av säkerhetsskyddsklassificerade uppgifter ska upphovsmannen tilldela dem en lämplig säkerhetsskyddsklassificeringsnivå 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 säkerhetsskyddsklassificeringsnivån. Dessa uppgifter ska ges till enheten för sekretessbelagda uppgifter när handlingarna lämnas in till denna enhet.

3. ”Andra sekretessbelagda uppgifter” som omfattas av tystnadsplikt ska hanteras i enlighet med bilagorna I och II och hanteringsanvisningarna.

Artikel 5

Europaparlamentets mottagande av sekretessbelagda uppgifter

1. Sekretessbelagda uppgifter som Europaparlamentet tar emot ska,

a) när det gäller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande, och ”andra sekretessbelagda uppgifter”, lämnas till sekretariatet för den parlamentsinstans eller befattningshavare inom parlamentet som har begärt uppgifterna, eller direkt till enheten för sekretessbelagda uppgifter,

b) när det gäller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande, lämnas till enheten för sekretessbelagda uppgifter.

2. Registrering, lagring och spårande av sekretessbelagda uppgifter ska allt efter omständigheterna säkerställas antingen av sekretariatet för den parlamentsinstans eller befattningshavare som har mottagit uppgifterna, eller av enheten för sekretessbelagda uppgifter.

3. De avtalade arrangemang som ska fastställas genom gemensamma överenskommelser i syfte att bevara uppgifternas sekretess, ska, när det gäller sekretessbelagda uppgifter som kommissionen lämnar enligt punkt 3.2 i bilaga 2 till ramavtalet eller säkerhetsskyddsklassificerade uppgifter som rådet vidarebefordrar i enlighet med artikel 5.4 i det interinstitutionella avtalet, allt efter omständigheterna lämnas in tillsammans med de sekretessbelagda uppgifterna antingen till sekretariatet för den berörda parlamentsinstansen/befattningshavaren eller till enheten för sekretessbelagda uppgifter.

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. För att säkerställa ett skydd som motsvarar säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska talmanskonferensen tillsätta ett tillsynsutskott. Uppgifter som har klassificerats som TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska meddelas Europaparlamentet enligt ytterligare arrangemang som ska avtalas mellan Europaparlamentet och den EU-institution som lämnar uppgifterna i fråga.

Artikel 6

Europaparlamentets lämnande av säkerhetsskyddsklassificerade uppgifter till tredje part

Europaparlamentet får med skriftligt förhandssamtycke från upphovsmannen eller från den unionsinstitution som lämnat de säkerhetsskyddsklassificerade uppgifterna till Europaparlamentet, allt efter omständigheterna, överlämna sådana säkerhetsskyddsklassificerade uppgifter till tredje part, under förutsättning att dessa parter ser till att bestämmelserna i detta beslut följs inom deras avdelningar och i deras lokaler när uppgifterna hanteras.

Artikel 7

Säkra utrymmen

1. För förvaltningen av sekretessbelagda uppgifter ska Europaparlamentet inrätta ett säkert område och säkra läsrum.

2. Det säkra området ska erbjuda resurser för registrering, konsultation, arkivering, överföring och hantering av säkerhetsskyddsklassificerade uppgifter. Det ska bland annat omfatta ett läsrum och ett sammanträdesrum där säkerhetsskyddsklassificerade uppgifter kan konsulteras, och det ska förvaltas av enheten för sekretessbelagda uppgifter.

3. Utanför det säkra området får säkra läsrum inrättas för konsultation av uppgifter som säkerhetsskyddsklassificerats upp till nivån RESTREINT UE/EU RESTRICTED eller motsvarande, och av ”andra sekretessbelagda uppgifter”. Dessa säkra läsrum ska förvaltas av de ansvariga avdelningarna inom sekretariaten för parlamentets instanser respektive befattningshavare, eller av enheten för sekretessbelagda uppgifter, allt efter omständigheterna. Rummen får inte innehålla kopieringsmaskiner, telefoner, faxmöjligheter, skannrar eller annan teknisk utrustning för reproduktion eller överföring av handlingar.

Artikel 8

Registrering, hantering och lagring av sekretessbelagda uppgifter

1. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” ska registreras och lagras av de ansvariga avdelningarna inom sekretariaten för den berörda parlamentsinstansen/befattningshavaren eller av enheten för sekretessbelagda uppgifter, beroende på vem som mottagit uppgifterna.

2. Följande villkor ska gälla för hantering av uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT EU/EU RESTRICTED eller motsvarande och för ”andra sekretessbelagda uppgifter”:

a) Handlingarna ska överlämnas personligen till sekretariatets chef, som ska registrera dem och utfärda ett mottagningsbevis.

b) När handlingarna inte används ska de förvaras i ett låst utrymme under sekretariatets ansvar.

c) Inte i något fall får uppgifterna sparas på något annat medium eller överföras till någon person. Handlingarna får endast kopieras med hjälp av utrustning som vederbörligen ackrediterats i enlighet med säkerhetsmeddelandena.

d) Tillgången till sådana uppgifter ska vara begränsad till de adressater som upphovsmannen angett eller till dem som angetts av den unionsinstitution som lämnat uppgifterna till Europaparlamentet, i enlighet med de arrangemang som avses i artikel 4.2 eller artikel 5.3, 5.4 och 5.5.

e) Parlamentsinstansens/befattningshavarens sekretariat ska föra ett register över de personer som har konsulterat handlingarna, med angivande av datum och klockslag för när detta skedde och ska överlämna registret till enheten för sekretessbelagda uppgifter när uppgifterna lämnas in till denna enhet.

3. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande, ska registreras, hanteras och lagras av enheten för sekretessbelagda uppgifter inom det säkra området, i överensstämmelse med den specifika säkerhetsskyddsklassificeringsnivån och i enlighet med säkerhetsmeddelandena.

4. Om reglerna i punkterna 1-3 inte följs ska ansvarig tjänsteman vid parlamentsorganets/befattningshavarens sekretariat eller vid enheten för sekretessbelagda uppgifter, allt efter omständigheterna, informera generalsekreteraren, som ska hänvisa frågan till talmannen om en ledamot i Europaparlamentet berörs.

Artikel 9

Tillträde till säkra utrymmen

1. Endast följande personer ska ha tillträde till det säkra området:

a) Personer som enligt artikel 3.4 –3.7 har förklarats behöriga att konsultera uppgifter där och som har lämnat in en ansökan i enlighet med artikel 10.1.

b) Personer som enligt artikel 4.1 har förklarats behöriga att framställa säkerhetsskyddsklassificerade uppgifter och som har lämnat in en ansökan i enlighet med artikel 10.1.

c) Tjänstemän vid Europaparlamentet som arbetar vid enheten för sekretessbelagda uppgifter.

d) Tjänstemän vid Europaparlamentet som ansvarar för förvaltningen av kommunikations- och informationssystemen.

e) När så krävs, de tjänstemän vid Europaparlamentet som ansvarar för säkerhet och brandsäkerhet.

f) Städpersonal, dock endast i närvaro och under noggrann uppsikt av en tjänsteman som arbetar vid enheten för sekretessbelagda uppgifter.

2. Enheten för sekretessbelagda uppgifter har befogenhet att neka varje person som inte är behörig tillträde till det säkra området. Invändningar mot ett sådant nekande av tillträde ska göras till talmannen, när det är Europaparlamentets ledamöter som begärt tillträde, och i övriga fall till generalsekreteraren.

3. Generalsekreteraren får bevilja att ett begränsat antal personer håller möte i det sammanträdesrum som är beläget inom det säkra området.

4. Endast följande personer ska ha tillträde till ett säkert läsrum:

a) Europaparlamentets ledamöter, tjänstemän vid Europaparlamentet och övriga anställda vid Europaparlamentet som arbetar för de politiska grupperna, med vederbörligt identifierat syfte att konsultera eller framställa sekretessbelagda uppgifter.

b) De tjänstemän vid Europaparlamentet som ansvarar för förvaltningen av kommunikations- och informationssystemen, tjänstemän vid sekretariatet för den parlamentsinstans eller befattningshavare som har mottagit uppgifterna och tjänstemän vid enheten för sekretessbelagda uppgifter.

c) När så krävs, de tjänstemän vid Europaparlamentet som ansvarar för säkerhet och brandsäkerhet.

d) Städpersonal, dock endast i närvaro och under noggrann uppsikt av en tjänsteman som arbetar vid parlamentsinstansens/befattningshavarens sekretariat eller vid enheten för sekretessbelagda uppgifter, allt efter omständigheterna.

5. Parlamentsinstansens eller befattningshavarens ansvariga sekretariat, eller enheten för sekretessbelagda uppgifter, allt efter omständigheterna, får neka alla obehöriga personer tillträde till ett säkert läsrum. Invändningar mot ett sådant nekande av tillträde ska göras till talmannen, när det är Europaparlamentets ledamöter som begärt tillträde, och i övriga fall till generalsekreteraren.

Artikel 10

Konsultation eller framställande av sekretessbelagda uppgifter i säkra utrymmen

1. Varje person som önskar konsultera eller framställa sekretessbelagda uppgifter i det säkra området ska i förväg lämna sitt namn till enheten för sekretessbelagda uppgifter. Enheten för sekretessbelagda uppgifter ska kontrollera identiteten för den personen och kontrollera om han eller hon är behörig att konsultera eller framställa sekretessbelagda uppgifter i enlighet med artikel 3.3 –3.7, artikel 4.1 eller artikel 5.3 –5.5.

2. Varje person som i enlighet med artikel 3.3 och 3.7 vill konsultera sekretessbelagda uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT EU/EU RESTRICTED eller motsvarande eller ”andra sekretessbelagda uppgifter” i ett säkert läsrum, ska i förväg lämna sitt namn till ansvarig avdelning vid parlamentsinstansens/befattningshavarens sekretariat eller till enheten för sekretessbelagda uppgifter.

3. Förutom i undantagsfall (t.ex. när många ansökningar om tillgång till uppgifter har lämnats in under en kort tid) får bara en person åt gången konsultera sekretessbelagda uppgifter i ett säkert utrymme i närvaro av en tjänsteman från parlamentsinstansens eller befattningshavarens sekretariat eller från enheten för sekretessbelagda uppgifter.

4. Under den tid som uppgifterna konsulteras får ingen kontakt med omvärlden förekomma (inbegripet via telefon eller annan teknisk utrustning). Det är förbjudet att göra anteckningar, och de konsulterade sekretessbelagda uppgifterna får inte kopieras eller fotograferas.

5. Innan en person tillåts lämna det säkra utrymmet ska tjänstemannen från parlamentsinstansens/befattningshavarens sekretariat eller från enheten för sekretessbelagda uppgifter försäkra sig om att de konsulterade sekretessbelagda handlingarna är kvar och kontrollera att de är intakta och fullständiga.

6. Om ovanstående regler inte följs ska tjänstemannen från parlamentsinstansens eller befattningshavarens sekretariat eller från enheten för sekretessbelagda uppgifter informera generalsekreteraren, som ska hänvisa ärendet till talmannen om en ledamot i Europaparlamentet berörs.

Artikel 11

Miniminormer för konsultation av sekretessbelagda uppgifter vid sammanträden inom stängda dörrar utanför de säkra utrymmena

1. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT EU/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” får konsulteras av parlamentsutskottens ledamöter eller av Europaparlamentets övriga politiska och administrativa organ vid sammanträden inom stängda dörrar utanför de säkra utrymmena.

2. När förutsättningarna enligt punkt 1 ovan föreligger ska sekretariatet för den parlamentsinstans eller den befattningshavare inom parlamentet som ansvarar för sammanträdet se till att följande regler följs:

a) Endast de personer som ordföranden för det behöriga utskottet eller organet kallat till sammanträdet får släppas in i sammanträdesrummet.

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

c) Protokollet från sammanträdet ska inte redogöra för innehållet i diskussioner om de uppgifter som behandlats. Endast det beslut som eventuellt fattas får föras till protokollet.

d) För sekretessbelagda uppgifter som muntligen meddelats mottagare i Europaparlamentet gäller en säkerhetsskyddsnivå motsvarande den som tillämpas på skriftliga sekretessbelagda uppgifter.

e) Inga extra exemplar av handlingar finnas i sammanträdesrummen.

f) Endast det antal handlingar som är nödvändigt delas ut till deltagare och tolkar vid sammanträdets början.

g) När sammanträdet inleds klargör mötets ordförande vilken säkerhetsskyddsklassificering/markeringsstatus som gäller för handlingarna.

h) Deltagarna tar inte med några handlingar ut ur sammanträdesrummet.

i) Alla exemplar av handlingarna samlas in, och vid sammanträdets slut tar parlamentsinstansens eller befattningshavarens sekretariat hand om dem och ser till att ingenting saknas.

j) Ingen elektronisk kommunikationsutrustning eller annan elektronisk utrustning får förekomma i det sammanträdesrum där de sekretessbelagda uppgifterna konsulteras eller diskuteras.

3. När, i överensstämmelse med de undantag som fastställs i punkt 3.2.2 i bilaga II till ramavtalet och i artikel 6.4 i det interinstitutionella avtalet, uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande diskuteras vid ett sammanträde inom stängda dörrar, ska sekretariatet för den parlamentsinstans/befattningshavare som ansvarar för sammanträdet, utöver bestämmelserna i punkt 2, se till att de personer som kallas att närvara vid sammanträdet uppfyller kraven i artikel 3.4 och 3.7.

4. I det fall som avses i punkt 3 ska enheten för sekretessbelagda uppgifter överlämna det antal exemplar som behövs av de handlingar som ska diskuteras till sekretariatet för den parlamentsinstans/befattningshavare som ansvarar för sammanträdet. Efter sammanträdet ska alla exemplar av handlingarna återlämnas till enheten för sekretessbelagda uppgifter.

Artikel 12

Arkivering av sekretessbelagda uppgifter

1. Inom det säkra området ska det finnas ett säkert arkiveringssystem. Enheten för sekretessbelagda uppgifter ska ansvara för förvaltningen av säkerhetsarkivet i enlighet med normal arkiveringsstandard.

2. Säkerhetsskyddsklassificerade uppgifter som har lämnats in för slutförvaring hos enheten för sekretessbelagda uppgifter och uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT EU/EU RESTRICTED eller motsvarande och lämnats till parlamentsinstansens eller befattningshavarens sekretariat ska överföras till säkerhetsarkivet i det säkra området sex månader efter det att de senast konsulterats, dock senast ett år efter det att de lämnats in. ”Andra sekretessbelagda uppgifter” ska, om de inte överlämnas till enheten för sekretessbelagda uppgifter, lämnas till den berörda parlamentsinstansens/befattningshavarens sekretariat i enlighet med de allmänna bestämmelserna om dokumenthantering.

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

a) Endast de personer vars namn, funktion eller befattning anges i den följehandling som fylls i då de sekretessbelagda uppgifterna lämnas in ska tillåtas konsultera dessa uppgifter.

b) En ansökan om att få konsultera sekretessbelagda uppgifter ska lämnas till enheten för sekretessbelagda uppgifter, som ska överföra berörda handlingar till det säkra läsrummet.

c) De regler och förfaranden som anges i artikel 10 om konsultation av sekretessbelagda uppgifter ska tillämpas.

Artikel 13

Placering på en lägre säkerhetsskyddsklassificeringsnivå, beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade och avmarkering av sekretessbelagda uppgifter

1. Sekretessbelagda uppgifter kan placeras på en lägre säkerhetsskyddsklassificeringsnivå eller avmarkeras endast med upphovsmannens ***förhandssamtycke*** och, om så krävs, efter diskussion med andra berörda parter.

2. Placering på en lägre säkerhetsskyddsklassificeringsnivå eller beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade ska bekräftas skriftligen. Upphovsmannen är ansvarig för att informera uppgifternas mottagare om ändringen, och dessa är i sin tur ansvariga för att lämna vidare informationen till eventuella efterföljande mottagare till vilka de har översänt handlingen eller en kopia av den. Om det är möjligt ska upphovsmännen, på de sekretessbelagda handlingarna, ange ett datum, en tidsperiod eller en händelse när uppgifterna får placeras på en lägre säkerhetsskyddsklassificeringsnivå eller när uppgifterna inte längre ska vara säkerhetsskyddsklassificerade. I annat fall ska upphovsmännen se över handlingarna minst vart femte år för att förvissa sig om att den ursprungliga säkerhetsskyddsklassificeringen fortfarande är nödvändig.

3. Sekretessbelagda uppgifter som förvaras i de säkra arkiven ska behandlas i god tid, och senast den 25:e årsdagen efter det att de framställdes, för att man ska kunna besluta om uppgifterna inte längre ska vara säkerhetsskyddsklassificerade, om de ska placeras på en lägre säkerhetsskyddsklassificeringsnivå eller om de ska avmarkeras. Behandling och offentliggörande av sådana uppgifter ska ske 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]). Borttagandet av säkerhetsskyddsklassificeringen ska utföras av upphovsmannen till de säkerhetsskyddsklassificerade uppgifterna eller av den enhet som vid den aktuella tidpunkten är ansvarig enligt bilaga I del 1 punkt 10.

4. Efter det att säkerhetsskyddsklassificeringen tagits bort ska tidigare säkerhetsskyddsklassificerade uppgifter som förvarats i det säkra arkivet överföras till Europaparlamentets historiska arkiv för permanent bevarande och vidare behandling enligt tillämpliga bestämmelser.

5. Efter att ha avmarkerats ska ”andra sekretessbelagda uppgifter” behandlas enligt Europaparlamentets bestämmelser om dokumenthantering.

Artikel 14

Överträdelser av säkerhetsbestämmelserna och förlust eller röjande av sekretessbelagda uppgifter

1. En överträdelse av sekretessregler i allmänhet och av detta beslut i synnerhet ska, när det gäller Europaparlamentets ledamöter, medföra tillämpning av relevanta bestämmelser avseende påföljder som fastställs i Europaparlamentets arbetsordning.

2. En överträdelse som begås av en av Europaparlamentets anställda ska medföra 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*).

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

3. Talmannen och/eller generalsekreteraren, allt efter omständigheterna, ska låta genomföra de eventuella utredningar som krävs, om det sker en överträdelse enligt definitionen i säkerhetsmeddelande 6.

4. Om de sekretessbelagda uppgifterna lämnats till Europaparlamentet av en annan unionsinstitution eller av en medlemsstat ska talmannen och/eller generalsekreteraren, allt efter omständigheterna, informera den berörda unionsinstitutionen eller medlemsstaten om varje förlust eller röjande av säkerhetsskyddsklassificerade uppgifter som misstänks eller som bevisligen har skett och om utredningens resultat samt om de åtgärder som vidtagits för att förhindra att situationen upprepas.

Artikel 15

Anpassning av detta beslut och dess genomförandebestämmelser och årlig rapportering om tillämpningen av detta beslut

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

2. Generalsekreteraren ska ansvara för att Europaparlamentets avdelningar tillämpar detta beslut och utfärda hanteringsanvisningar för frågor som omfattas av ledningssystemet för informationssäkerhet i enlighet med de principer som fastställs genom detta beslut.

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

Artikel 16

Övergångsbestämmelser och slutbestämmelser

1. Uppgifter som inte är säkerhetsskyddsklassificerade och som innehas inom enheten för sekretessbelagda uppgifter eller i något annat av Europaparlamentets arkiv samt betraktas som sekretessbelagda och daterats före den 1 april 2014 ska vid tillämpningen av detta beslut anses utgöra ”andra sekretessbelagda uppgifter”. Upphovsmannen får när som helst ompröva dess sekretessnivå.

2. För en period på tolv månader från och med den 1 april 2014 ska, som ett undantag från artikel 5.1 a och från artikel 8.1 i detta beslut, uppgifter som lämnats av rådet i enlighet med det interinstitutionella avtalet och som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande överlämnas till och registreras och lagras av enheten för sekretessbelagda uppgifter. Uppgifterna får konsulteras i enlighet med artiklarna 4.2 a, 4.2 c och 5.4 i det interinstitutionella avtalet.

3. Europaparlamentets presidiums beslut av den 6 juni 2011 om bestämmelserna för Europaparlamentets hantering av sekretessbelagda uppgifter upphävs härmed.

Artikel 17

Ikraftträdande

Detta beslut träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

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 för skydd av sekretessbelagda uppgifter som ska följas av Europaparlamentet på alla dess anställningsorter, samt av alla mottagare av säkerhetsskyddsklassificerade uppgifter och ”andra sekretessbelagda uppgifter”, så att säkerheten garanteras och berörda personer kan vara förvissade om att det råder en gemensam standard för skyddet. Bestämmelserna åtföljs av de säkerhetsmeddelanden som återfinns i bilaga II och av andra föreskrifter om hur parlamentsutskotten och andra parlamentsinstanser eller befattningshavare inom parlamentet ska behandla sekretessbelagda uppgifter.

2. **GRUNDLÄGGANDE PRINCIPER**

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

Laglighet innebär att man strikt måste hålla sig inom de rättsliga ramarna i fullgörandet av säkerhetsfunktioner och följa tillämpliga rättslig krav. Dessutom måste allt ansvar på säkerhetsområdet grundas 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 ska överträdelser av säkerhetsbestämmelserna inom Europaparlamentets ansvarsområden hanteras på ett sätt som överensstämmer med dess arbetsordning och dess policy för disciplinära åtgärder.

Öppenhet och insyn innebär ett behov av tydlighet avseende alla säkerhetsbestämmelser och säkerhetsföreskrifter för att skapa balans mellan olika tjänster och olika områden (fysisk säkerhet jämfört med informationsskydd osv.) och uppnå en konsekvent och strukturerad policy för säkerhetstänkande. Dessutom är tydliga skriftliga riktlinjer nödvändiga för genomförandet av säkerhetsåtgärderna.

Ansvarsskyldighet innebär att ansvarsförhållanden på säkerhetsområdet måste definieras tydligt. Dessutom innebär det ett behov av att regelbundet övervaka om ansvarskraven har efterlevts på korrekt sätt.

Subsidiaritet innebär att säkerheten måste organiseras på lägsta möjliga nivå och så nära Europaparlamentets generaldirektorat och enheter som möjligt. Proportionalitet innebär att säkerhetsverksamheterna strikt måste begränsas till de som är absolut nödvändiga och att säkerhetsåtgärderna måste 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) Det finns lämpliga kommunikations- och informationssystem. Dessa omfattas av Europaparlamentets säkerhetsmyndighets ansvar (enligt säkerhetsmeddelande 1).

b) I Europaparlamentet ansvarar myndigheten för informationssäkring för att i samarbete med den berörda säkerhetsmyndigheten tillhandahålla information och ge råd om tekniska hot mot kommunikations- och informationssystem och om vilka skyddsåtgärder som kan vidtas för att motverka hoten.

c) Europaparlamentets ansvariga enheter och övriga EU-institutioners säkerhetstjänster bedriver ett nära samarbete.

4. **PRINCIPER FÖR INFORMATIONSSÄKERHET**

4.1. ***Mål***

Informationssäkerhetens huvudsyften är

a) att skydda *sekretessbelagda uppgifter* mot spionerі, överträdelser av säkerhetsbestämmelserna och röjande utan tillstånd,

b) att skydda säkerhetsskyddsklassificerade uppgifter som hanteras i kommunikations- och informationssystem och i motsvarande nätverk mot hot som riktar sig mot uppgifternas sekretess, integritet och tillgänglighet,

c) att skydda Europaparlamentets lokaler där säkerhetsskyddsklassificerade uppgifter förvaras mot sabotage och uppsåtlig skadegörelse,

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

4.2. ***Säkerhetsskyddsklassificering***

4.2.1. I sekretessfrågor krävs omsorg och erfarenhet vid valet av vilka uppgifter och vilket material som ska skyddas, liksom vid bedömningen av vilken skyddsnivå som krävs. Grundläggande är att skyddsnivån ska motsvara hur känsliga de enskilda uppgifterna eller det material som ska skyddas är, sett ur ett säkerhetsperspektiv. För att säkerställa ett smidigt informationsflöde ska man undvika att placera uppgifter på en alltför hög säkerhetsskyddsklassificeringsnivå såväl som på en alltför låg.

4.2.2. Systemet för säkerhetsskyddsklassificering är det instrument som ska användas för att praktiskt tillämpa de principer som fastställs i detta avsnitt. Ett liknande system för säkerhetsskyddsklassificering ska följas vid planering och organisering av arbetet mot spionerі, sabotage, terrorism och andra hot, så att de viktigaste lokalerna där säkerhetsskyddsklassificerade uppgifter förvaras och de känsligaste utrymmena inom dessa får högsta möjliga skyddsnivå.

4.2.3. Ansvaret för säkerhetsskyddsklassificeringen av uppgifter ligger enbart hos uppgifternas upphovsmän.

4.2.4. Säkerhetsskyddsklassificeringsnivån ska grunda sig endast på de berörda uppgifternas innehåll.

4.2.5. När ett antal uppgifter som grupperats tillsammans ska säkerhetsskyddsklassificeras ska deras placering göras på en nivå som är minst lika hög som den högsta nivån som tilldelats en av dess delar. En samlad grupp uppgifter får dock placeras på en högre säkerhetsskyddsklassificeringsnivå än de enskilda uppgifter som ingår i gruppen.

4.2.6. Uppgifter ska säkerhetsskyddsklassificeras endast när det är nödvändigt och för så lång tid som behövs.

4.3. ***Säkerhetsåtgärdernas syfte***

Säkerhetsåtgärderna ska

a) omfatta alla personer som har tillgång till säkerhetsskyddsklassificerade uppgifter, medier med säkerhetsskyddsklassificerade uppgifter och ”andra sekretessbelagda uppgifter” samt utrymmen där sådana uppgifter förvaras och där viktiga anläggningar finns,

b) vara utformade så att personer identifieras vars ställning (i fråga om tillträdesmöjligheter, relationer eller annat) 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 till 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 (genom att förebygga förvanskning, obehörig ändring eller obehörig radering) och tillgängligheten (för dem som behöver och är behöriga att få tillgång till uppgifterna) till alla sekretessbelagda uppgifter, oavsett om de är säkerhetsskyddsklassificerade eller inte, särskilt för sådana uppgifter som lagras, bearbetas eller överförs i elektromagnetisk form.

5. GEMENSAMMA MINIMINORMER

Europaparlamentet ska se till att gemensamma miniminormer för säkerhet följs av alla mottagare av säkerhetsskyddsklassificerade uppgifter, både inom institutionen och under dess befogenhet, inbegripet alla dess instanser 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, och förfaranden för skydd av sekretessbelagda uppgifter.

Europaparlamentet får tillåta att sådana uppgifter vidarebefordras till tredje part endast om dessa parter kan garantera att de följer föreskrifter som minst motsvarar dessa gemensamma miniminormer när de hanterar uppgifterna.

Sådana gemensamma miniminormer ska också tillämpas när Europaparlamentet enligt kontrakt eller bidragsöverenskommelser tilldelar företag eller andra enheter uppdrag som involverar sekretessbelagda uppgifter.

6. SÄKERHETEN AVSEENDE EUROPAPARLAMENTETS TJÄNSTEMÄN OCH ÖVRIGA ANSTÄLLDA VID PARLAMENTET SOM ARBETAR FÖR DE POLITISKA GRUPPERNA

6.1. *Säkerhetsanvisningar avseende 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 i positioner som innebär att de kan få tillgång till säkerhetsskyddsklassificerade uppgifter, ska, både när de börjar sin tjänst och därefter med jämna mellanrum, ges noggranna anvisningar avseende säkerhetskraven och de förfaranden som måste följas för att denna säkerhet ska uppnås. Dessa personer ska skriftligen bekräfta att de har läst och till fullo förstått tillämpliga säkerhetsbestämmelser.

6.2. *Ledningsansvar*

Det måste ingå i arbetsledningens uppgifter att känna till vilka i personalen som arbetar med säkerhetsskyddsklassificerade uppgifter eller har tillgång till säkra kommunikations- eller informationssystem, och registrera samt rapportera incidenter eller uppenbara svaga punkter som skulle kunna påverka säkerheten.

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

Förfaranden ska fastställas för att säkerställa att det, när det kommer fram oroväckande information om en av Europaparlamentets tjänstemän eller någon övrig anställd vid parlamentet som arbetar för en politisk grupp, vidtas åtgärder för att fastställa huruvida denna persons arbete innebär kontakt med säkerhetsskyddsklassificerade uppgifter eller huruvida han eller hon har tillgång till säkra kommunikations- eller informationssystem, samt att Europaparlamentets ansvariga instanser informeras. Om den behöriga nationella säkerhetsmyndigheten anger att personen i fråga utgör en säkerhetsrisk ska han eller hon avstängas eller avlägsnas från uppdrag där säkerheten skulle kunna äventyras.

7. FYSISK SÄKERHET

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

7.1. ***Behov av skydd***

Den grad av fysiska säkerhetsåtgärder som ska tillämpas för att skydda säkerhetsskyddsklassificerade uppgifter ska stå i proportion till säkerhetsskyddsklassificeringsnivån för och omfattningen av och hotet mot uppgifterna och materialet. Alla som har tillgång till säkerhetsskyddsklassificerade uppgifter ska tillämpa enhetliga rutiner för säkerhetsskyddsklassificering 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 säkerhetsskyddsklassificerade uppgifter lämnar utrymmen med sådana uppgifter obevakade 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 säkerhetsskyddsklassificerade uppgifter förvaras eller där det finns skyddade kommunikations- eller informationssystem ska skyddas mot obehörigt tillträde.

Arten av skydd för säkerhetsskyddsklassificerade 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 av

a) säkerhetsskyddsklassificeringsnivån för och omfattningen av de uppgifter och det material som ska skyddas samt var i byggnaden uppgifterna och materialet 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 överträdelser av säkerhetsbestämmelserna, 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 säkerhetsskyddsklassificerade uppgifter ska skyddas i händelse av en nödsituation.

8. **SÄKERHETSBETECKNINGAR, MARKERINGAR, FASTSÄTTANDE OCH HANTERING AV SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅER**

8.1. ***Säkerhetsbeteckningar***

Inga andra säkerhetsskyddsklassificeringsnivåer än de som definieras i artikel 2 d i detta beslut är tillåtna.

För att begränsa en säkerhetsskyddsklassificeringsnivås giltighet (för säkerhetsskyddsklassificerade uppgifter som innebär en automatisk placering på en lägre säkerhetsskyddsklassificeringsnivå eller beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade) får en överenskommen säkerhetsbeteckning användas.

Säkerhetsbeteckningar ska endast användas tillsammans med en säkerhetsskyddsklassificeringsnivå.

Säkerhetsbeteckningarna regleras ytterligare i säkerhetsmeddelande 2 och definieras i hanteringsanvisningarna.

8.2. ***Markeringar***

En markering ska användas för att ange specifika förhandsanvisningar om hanteringen av sekretessbelagda uppgifter. En markering får också användas för att ange vilket område en viss handling omfattar eller särskild spridning, grundad på behov av kännedom i tjänsten, eller (för icke-säkerhetsskyddsklassificerade uppgifter) för att markera slutet på ett handelsförbud.

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

Markeringarna regleras ytterligare i säkerhetsmeddelande 2 och definieras i hanteringsanvisningarna.

8.3. ***Fastsättande av säkerhetsskyddsklassificeringsnivåer och säkerhetsbeteckningar***

Fastsättande av säkerhetsskyddsklassificeringsnivåer och säkerhetsbeteckningar och markeringar ska ske i enlighet med säkerhetsmeddelande 2 avsnitt E och med hanteringsanvisningarna.

8.4. ***Hantering av säkerhetsskyddsklassificeringsnivåer***

8.4.1 *Allmänt*

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

Ansvaret för att säkerhetsskyddsklassificera uppgifter och för en eventuell senare placering på en lägre säkerhetsskyddsklassificeringsnivå eller för beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade vilar helt på upphovsmannen.

Europaparlamentets tjänstemän ska säkerhetsskyddsklassificera uppgifter, placera dem på en lägre säkerhetsskyddsklassificeringsnivå eller besluta om att de inte längre ska vara säkerhetsskyddsklassificerade på uppdrag av eller genom delegering från generalsekreteraren.

De detaljerade förfarandena för hantering av säkerhetsskyddsklassificerade 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 uppgifter som placeras på säkerhetsskyddsklassificeringsnivån 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 sekretessbelagda uppgifter.

8.4.2 *Tillämpning av säkerhetsskyddsklassificering*

Säkerhetsskyddsklassificering av en handling ska fastställas med utgångspunkt i hur känsligt handlingens innehåll är, i enlighet med definitionerna i artikel 2 c. Det är viktigt att säkerhetsskyddsklassificeringar tilldelas korrekt och används sparsamt.

Säkerhetsskyddsklassificeringsnivån för en skrivelse eller en not som åtföljs av bilagor ska vara åtminstone densamma som den högsta säkerhetsskyddsklassificeringsnivå som tilldelats en av bilagorna. Upphovsmannen ska tydligt ange med vilken säkerhetsskyddsklassificeringsnivå skrivelsen eller noten ska förses när den skilts från de bifogade handlingarna.

Upphovsmannen till en handling som ska säkerhetsskyddsklassificeras ska följa ovanstående bestämmelser och undvika varje tendens att placera handlingen på en alltför hög respektive låg säkerhetsskyddsklassificeringsnivå.

Enstaka sidor, stycken, avsnitt, bilagor, tillägg och bifogade ark till en viss handling kan kräva placering på en annan säkerhetsskyddsklassificeringsnivå och ska säkerhetsskyddsklassificeras i enlighet med detta. Säkerhetsskyddsklassificeringsnivån för handlingen som helhet ska vara densamma som den del som fått den högsta säkerhetsskyddsklassificeringsnivån.

9. **INSPEKTIONER**

Periodiska interna inspektioner av säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade uppgifter ska utföras av Europaparlamentets direktorat för säkerhet och riskbedömning, som kan begära stöd av rådets eller kommissionens säkerhetsmyndigheter.

Säkerhetsmyndigheterna och de behöriga avdelningarna vid unionsinstitutionerna får, som en del av en överenskommen process inledd av någon av parterna, genomföra utvärderingar korsvis av varandras säkerhetsarrangemang för skydd av säkerhetsskyddsklassificerade uppgifter som ingår i utbyten enligt de relevanta interinstitutionella avtalen.

10. **FÖRFARANDEN FÖR BESLUT OM ATT UPPGIFTER INTE LÄNGRE SKA VARA SÄKERHETSSKYDDSKLASSIFICERADE OCH FÖR AVMARKERING**

10.1. Enheten för sekretessbelagda uppgifter ska granska sekretessbelagda uppgifter som ingår i dess register och söka upphovsmannens samtycke till beslut om att en handling inte längre ska vara säkerhetsskyddsklassificerad eller till avmarkering av handlingen allra senast på 25-årsdagen från dess upprättande. Handlingar för vilka beslut inte fattats om att de inte längre ska vara säkerhetsskyddsklassificerade eller som inte avmarkerats vid den första granskningen ska regelbundet, dock minst vart femte år, granskas på nytt. Förutom på handlingar som fysiskt befinner sig i säkerhetsarkivet i det säkra området och som säkerhetsskyddsklassificerats i vederbörlig ordning får avmarkeringsförfarandet också tillämpas på andra sekretessbelagda uppgifter som finns antingen av parlamentsinstansen/befattningshavaren eller inom den avdelning som ansvarar för parlamentets historiska arkiv.

10.2 Beslutet om att en handling inte längre ska vara säkerhetsskyddsklassificerad eller om avmarkering av en handling ska som en allmän regel fattas uteslutande av upphovsmannen eller, i undantagsfall, i samarbete med den parlamentsinstans/befattningshavare som innehar sådana uppgifter, innan de uppgifter som handlingen i fråga innehåller överförs till den avdelning som ansvarar för parlamentets historiska arkiv. Beslut om att säkerhetsskyddsklassificerade uppgifter inte längre ska vara säkerhetsskyddsklassificerade eller om avmarkering av säkerhetsskyddsklassificerade uppgifter får endast fattas med efter skriftligt samtycke från upphovsmannen. För ”andra sekretessbelagda uppgifter” ska sekretariatet vid den parlamentsinstans/befattningshavare som innehar sådana uppgifter i samarbete med upphovsmannen besluta huruvida handlingen kan avmarkeras.

10.3. Enheten för sekretessbelagda uppgifter ska i upphovsmannens ställe ha ansvaret för att informera handlingens mottagare om förändringen av säkerhetsskyddsklassificeringsnivån eller markeringen, 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 beslut om att säkerhetsskyddsklassificerade uppgifter inte längre ska vara säkerhetsskyddsklassificerade ska inte påverka eventuella säkerhetsbeteckningar eller markeringar som kan finnas i handlingen.

10.5. Vid beslut om att säkerhetsskyddsklassificerade uppgifter inte längre ska vara säkerhetsskyddsklassificerade ska den ursprungliga säkerhetsskyddsklassificeringsnivån, som är angiven upptill och nedtill på varje sida, strykas över. Första sidan (försättsbladet) i handlingen ska stämplas och förses med en referensuppgift från enheten för sekretessbelagda uppgifter. Vid avmarkering ska den ursprungliga markeringen, som är angiven upptill och nedtill på varje sida, strykas över.

10.6. Texten till den handling för vilken beslut fattats om att den inte längre ska vara säkerhetsskyddsklassificerad eller som avmarkerats 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 sekretessbelagda uppgifter samråda med denna tredje part innan beslut fattas om att handlingarna inte längre ska vara säkerhetsskyddsklassificerade eller om avmarkering.

b) När det gäller undantaget som rör den enskildes privatliv och personliga integritet ska förfarandet för att fatta beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade eller om avmarkering särskilt beakta om den berörda personen samtycker eller, allt efter omständigheterna, om det är omöjligt att fastställa identiteten för den berörda personen.

c) När det gäller undantaget som rör en fysisk eller juridisk persons affärsintressen får 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. För att få tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande ska Europaparlamentets ledamöter ha getts behörighet antingen i enlighet med det förfarande som avses i punkterna 11.3 och 11.4 i denna bilaga eller på grundval av en försäkran på heder och samvete att de inte kommer att röja uppgifterna i enlighet med artikel 3.4 i detta beslut.

11.2 För att få tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande måste ledamöterna ha getts behörighet i enlighet med det förfarande som avses i punkterna 11.3 och 11.14.

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 punkterna 11.9–11.14. Talmannen ska vara ansvarig för att bevilja ledamöterna behörighet.

11.4 Talmannen får skriftligen 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 för säkerhet och riskbedömning 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, beroende på vilket som är kortast. Den får förnyas i enlighet med det förfarande 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 den behöriga nationella myndigheten ange nivån på de säkerhetsskyddsklassificerade uppgifter som den berörda ledamoten i Europaparlamentet ska få tillgång till, så att den 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 myndighet avger ett positivt yttrande får talmannen bevilja den berörda ledamoten i Europaparlamentet behörighet.

11.13. Ett negativt yttrande från den behöriga nationella myndigheten 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 säkerhetsskyddsklassificerade uppgifter och hur detta skydd ska säkerställas. Dessa ledamöter ska underteckna en förklaring om att de mottagit dessa anvisningar.

11.15. Talmannen får i undantagsfall, efter att i förväg ha informerat den behöriga nationella myndigheten och förutsatt att inget svar mottagits från den myndigheten 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. Tillfällig behörighet som beviljas på detta sätt ska inte ge tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET eller motsvarande.

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 säkerhetsskyddsklassificerade uppgifter, får ha tillgång till sådana uppgifter.

12.2. För att få tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET, eller motsvarande måste berörda tjänstemän vid Europaparlamentet och övriga anställda vid Europaparlamentet som arbetar för de politiska grupperna 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 skriftligen 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 för säkerhet och riskbedömning 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 ska vara giltig för en period av fem år eller för den tid som uppgifterna, som låg till grund för att den beviljades, varar, beroende på vilket som är kortast. 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 tjänstemannen vid Europaparlamentet eller den anställde vid Europaparlamentet som arbetar för en politisk grupp 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 som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET.

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 den behöriga nationella myndigheten ange nivån på de säkerhetsskyddsklassificerade uppgifter som den berörda tjänstemannen vid Europaparlamentet eller den anställde vid Europaparlamentet som arbetar för en politisk grupp ska få tillgång till, så att den 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 myndighet avger ett positivt yttrande får generalsekreteraren bevilja den berörda tjänstemannen vid Europaparlamentet eller den anställde vid Europaparlamentet som arbetar för en politisk grupp behörighet.

12.13. Ett negativt yttrande från den behöriga nationella myndigheten 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 myndigheten. 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 punkterna 12.4 och 12.5 ska, när behörigheten beviljas och därefter med jämna mellanrum, erhålla alla nödvändiga anvisningar angående skyddet av säkerhetsskyddsklassificerade 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 inget svar mottagits från den myndigheten 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. Tillfälliga behörigheter som beviljas på detta sätt ska inte ge tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande.

BILAGA II

INLEDNING

Genom dessa bestämmelser fastställs de säkerhetsmeddelanden som styr och garanterar en säker behandling och hantering av sekretessbelagda uppgifter från Europaparlamentets sida. Dessa säkerhetsmeddelanden utgör tillsammans med hanteringsanvisningarna Europaparlamentets ledningssystem för informationssäkerhet, som avses i artikel 3.2 i detta beslut.

SÄKERHETSMEDDELANDE 1

Säkerhetsorganisationen inom Europaparlamentet för skydd av sekretessbelagda uppgifter

SÄKERHETSMEDDELANDE 2

Hantering av sekretessbelagda uppgifter

SÄKERHETSMEDDELANDE 3

Behandling av sekretessbelagda uppgifter med hjälp av automatiserade kommunikations- och informationssystem

SÄKERHETSMEDDELANDE 4

Fysisk säkerhet

SÄKERHETSMEDDELANDE 5

Industrisäkerhet

SÄKERHETSMEDDELANDE 6

Överträdelser av säkerhetsbestämmelserna och förlust eller röjande av sekretessbelagda uppgifter

SÄKERHETSMEDDELANDE 1

SÄKERHETSORGANISATIONEN INOM EUROPAPARLAMENTET FÖR SKYDD AV SEKRETESSBELAGDA UPPGIFTER

1. Generalsekreteraren ska ansvara för det övergripande och konsekventa genomförandet av detta beslut.

Generalsekreteraren ska vidta alla nödvändiga åtgärder vid hantering eller lagring av sekretessbelagda uppgifter för att garantera att detta beslut tillämpas i parlamentets lokaler, av Europaparlamentets ledamöter, av Europaparlamentets tjänstemän, av parlamentets övriga anställda som arbetar för de politiska grupperna och av uppdragstagare.

2. Generalsekreteraren är säkerhetsmyndigheten. I den egenskapen ska generalsekreteraren

2.1. samordna alla säkerhetsfrågor som avser skyddet av sekretessbelagda uppgifter som berör parlamentets verksamhet,

2.2. godkänna installationen av ett säkert område, säkra läsrum och säker utrustning,

2.3. genomföra beslut som i enlighet med artikel 6 i detta beslut tillåter att parlamentet överlämnar säkerhetsskyddsklassificerade uppgifter till tredje part,

2.4. undersöka eller låta undersöka eventuella läckor av sekretessbelagda uppgifter som tycks ha uppstått inom parlamentet, i samarbete med Europaparlamentets talman om en ledamot av Europaparlamentet berörs,

2.5. upprätthålla nära kontakt med säkerhetsmyndigheterna vid unionens övriga institutioner och med de nationella säkerhetsmyndigheterna i medlemsstaterna i syfte att garantera en optimal samordning av säkerhetsstrategier med koppling till säkerhetsskyddsklassificerade uppgifter,

2.6. se till att parlamentets säkerhetsstrategi och motsvarande förfaranden fortlöpande ses över och utfärda lämpliga rekommendationer till följd av detta,

2.7. rapportera till den nationella säkerhetsmyndighet som utfört säkerhetsprövningen i enlighet med bilaga I del 2 punkt 11.3, i fall som inbegriper negativa uppgifter som skulle kunna påverka den myndigheten.

3. Om en ledamot av Europaparlamentet berörs ska generalsekreteraren fullgöra sina skyldigheter i nära samarbete med Europaparlamentets talman.

4. Vid fullgörandet av sina skyldigheter enligt punkterna 2 och 3 ska generalsekreteraren bistås av den ställföreträdande generalsekreteraren, direktoratet för säkerhet och riskbedömning, direktoratet för informationsteknik och enheten för sekretessbelagda uppgifter.

4.1. Direktoratet för säkerhet och riskbedömning ska ansvara för personliga skyddsåtgärder och i synnerhet för förfarandet för säkerhetsprövning, såsom det fastställs i bilaga I del 2. Direktoratet för säkerhet och riskbedömning ska i även

a) vara kontaktpunkten för säkerhetsmyndigheterna vid unionens övriga institutioner och för de nationella säkerhetsmyndigheterna i frågor som rör förfaranden för säkerhetsprövning av Europaparlamentets ledamöter, av Europaparlamentets tjänstemän och av parlamentets övriga anställda som arbetar för de politiska grupperna,

b) ge nödvändig allmän säkerhetsinformation om skyldigheterna att skydda säkerhetsskyddsklassificerade uppgifter och om konsekvenserna av underlåtenhet att fullgöra dessa skyldigheter,

c) övervaka driften av det säkra området och de säkra läsrummen i parlamentets lokaler, vid behov i samarbete med övriga unionsinstitutioners och medlemsstaternas säkerhetstjänster,

d) i samarbete med övriga EU-institutioners och nationella säkerhetstjänster övervaka förfarandena för hantering och lagring av säkerhetsskyddsklassificerade uppgifter samt det säkra område och de säkra läsrum i parlamentets lokaler där säkerhetsskyddsklassificerade uppgifter hanteras,

e) föreslå lämpliga hanteringsanvisningar för generalsekreteraren.

4.2. Direktoratet för informationsteknik ska ansvara för hanteringen av sekretessbelagda uppgifter av säkra it-system inom Europaparlamentet.

4.3. Enheten för sekretessbelagda uppgifter ska ansvara för

a) att i nära samarbete med direktoratet för säkerhet och riskbedömning och direktoratet för informationsteknik och med övriga unionsinstitutioners säkerhetstjänster fastställa säkerhetsbehoven när det gäller ett effektivt skydd av sekretessbelagda uppgifter,

b) att fastställa alla aspekter av hantering och lagring av sekretessbelagda uppgifter inom parlamentet, i enlighet med hanteringsanvisningarna,

c) driften av det säkra området,

d) hanteringen eller konsultationen av sekretessbelagda uppgifter i det säkra området eller i det säkra läsrummet inom enheten för sekretessbelagda uppgifter, i enlighet med artikel 7.2 och 7.3 i detta beslut,

e) hanteringen av det register som enheten för sekretessbelagda uppgifter för,

f) att rapportera till säkerhetsmyndigheten om eventuella bevisade eller misstänkta överträdelser av säkerhetsbestämmelserna och om eventuell förlust eller eventuellt röjande av sekretessbelagda uppgifter som lämnats in till enheten för sekretessbelagda uppgifter och förvaras i det säkra området eller det säkra läsrummet inom enheten för sekretessbelagda uppgifter.

5. Vidare ska generalsekreteraren i egenskap av säkerhetsmyndighet utse följande myndigheter:

a) En ackrediteringsmyndighet för säkerhet.

b) En driftsansvarig myndighet för informationssäkring.

c) En krypteringsdistribuerande myndighet.

d) En tempestmyndighet.

e) En myndighet för informationssäkring.

Utövandet av dessa funktioner kräver inte separata organisatoriska enheter. De ska visserligen ha olika mandat men dessa funktioner, och deras medföljande ansvarsområden, får kombineras eller integreras i samma organisatoriska enhet eller delas upp i olika organisatoriska enheter, förutsatt att intressekonflikter och dubbelarbete undviks.

6. Ackrediteringsmyndigheten för säkerhet ska tillhandahålla rådgivning i fråga om alla säkerhetsfrågor som rör ackrediteringen av varje it-system och it-nätverk inom parlamentet och

6.1. garantera att kommunikations- och informationssystemen överensstämmer med relevanta säkerhetsstrategier och säkerhetsriktlinjer, tillhandahålla ett intyg som godkänner att kommunikations- och informationssystemen hanterar säkerhetsskyddsklassificerade uppgifter för att i driftsmiljön skydda dessa uppgifter upp till en fastställd säkerhetsskyddsklassificeringsnivå samt ange villkoren för ackrediteringen och de kriterier enligt vilka nytt godkännande krävs,

6.2. upprätta ett förfarande för säkerhetsackreditering i enlighet med relevanta strategier, med klart angivande av villkoren för godkännande av kommunikations- och informationssystem under myndighetens överinseende,

6.3. utarbeta en säkerhetsackrediteringsstrategi som anger av vilken detaljgrad för ackreditering som motsvarar den säkerhetsnivå som krävs,

6.4. granska och godkänna säkerhetsrelaterad dokumentation, inbegripet riskhantering och redovisning av kvarstående risker, kontrolldokumentering av genomförandet av säkerhet och säkra driftsmetoder samt säkerställa att detta överensstämmer med parlamentets säkerhetsbestämmelser och säkerhetsstrategier,

6.5. kontrollera genomförandet av säkerhetsåtgärder avseende kommunikations- och informationssystem genom att själv utföra eller stödja säkerhetsbedömningar, inspektioner och översyner,

6.6. fastställa säkerhetskrav (t.ex. nivåer för personalgodkännande) för känsliga befattningar inom kommunikations- och informationssystemen,

6.7. godkänna eller i tillämpliga fall delta i ett gemensamt godkännande av samtrafik mellan olika kommunikations- och informationssystem,

6.8. godkänna säkerhetsstandarderna för teknisk utrusning för säker hantering och skydd av säkerhetsskyddsklassificerade uppgifter,

6.9. se till att de kryptoprodukter som används inom parlamentet inkluderas i förteckningen över EU-godkända produkter,

6.10. samråda med systemleverantören, säkerhetsaktörerna och företrädare för användare när det gäller hantering av säkerhetsrisker, särskilt den kvarstående risken, och villkoren för redovisning av godkännandet.

7. Den driftsansvariga myndigheten för informationssäkring ska ansvara för att

7.1. utveckla säkerhetsdokumentation i linje med säkerhetsstrategier och säkerhetsriktlinjer, i synnerhet även redovisningen av den kvarstående risken, säkra driftsmetoder och krypteringsplanen inom ackrediteringsförfarandet för kommunikations- och informationssystemen,

7.2. delta i urval och tester av systemspecifika tekniska säkerhetsåtgärder, utrustning och programvara, för att övervaka genomförandet av dessa och se till att de installeras på ett säkert sätt, konfigureras och underhålls i enlighet med relevant säkerhetsdokumentation,

7.3. övervaka genomförande och tillämpning av säkra driftsmetoder och vid behov delegera säkerhetsansvaret för driften till systemägaren, nämligen enheten för sekretessbelagda uppgifter,

7.4. förvalta och hantera kryptoprodukter, och därvid säkerställa förvaringen av krypterat material och kontrollerat material samt, i förekommande fall, framställningen av kryptografiska variabler,

7.5. utföra översyner och tester av säkerhetsanalyser, särskilt för att ta fram relevanta riskrapporter, enligt kraven från ackrediteringsmyndigheten för säkerhet,

7.6. tillhandahålla kommunikationssystem- och informationssystemspecifik utbildning i informationssäkring,

7.7. genomföra och svara för driften av kommunikationssystem- och informationssystemspecifika säkerhetsåtgärder.

8. Kryptodistributionsmyndigheten ska ansvara för att

8.1. förvalta och redovisa EU-krypterat material,

8.2. i nära samarbete med ackrediteringsmyndigheten för säkerhet säkerställa att lämpliga förfaranden följs och att planer införs för redovisning, säker hantering, lagring och distribution av allt EU-krypterat material,

8.3. säkerställa överföring av EU-krypterat material till eller från enskilda personer eller enheter som använder detta.

9. Tempestmyndigheten ska ansvara för att kommunikations- och informationssystemen överensstämmer med tempeststrategierna och hanteringsanvisningarna. Den ska godkänna tempestmotåtgärder för anläggningar och produkter för att i driftsmiljön skydda säkerhetsskyddsklassificerade uppgifter upp till en fastställd säkerhetsskyddsklassificeringsnivå.

10. Myndigheten för informationssäkring ska ansvara för alla aspekter av förvaltningen och hanteringen av sekretessbelagda uppgifter inom parlamentet och i synnerhet för att

10.1 utveckla säkerheten och säkerhetsriktlinjer för informationssäkring och övervaka hur ändamålsenliga och relevanta dessa är,

10.2. skydda och administrera teknisk information som rör kryptoprodukter,

10.3. se till att de åtgärder för informationssäkring som väljs för skydd av säkerhetsskyddsklassificerade uppgifter överensstämmer med de relevanta strategierna för deras lämplighet och urval,

10.4. se till att kryptoprodukter väljs ut i överensstämmelse med strategin för deras lämplighet och urval,

10.5. samråda med systemleverantören, säkerhetsaktörerna och företrädarna för användare när det gäller säkerheten för informationssäkring,

SÄKERHETSMEDDELANDE 2

HANTERING AV SEKRETESSBELAGDA UPPGIFTER

A. **INLEDNING**

1. I detta säkerhetsmeddelande fastställs bestämmelserna om parlamentets hantering av sekretessbelagda uppgifter.

2. När sekretessbelagda uppgifter framställs ska upphovsmannen göra en bedömning av konfidentialitetsnivån och fatta ett beslut på grundval av de principer som fastställs i detta säkerhetsmeddelande när det gäller säkerhetsskyddsklassificering eller markering av uppgifterna i fråga.

B. **SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER**

3. Beslutet att säkerhetsskyddsklassificera en handling ska fattas innan den upprättas. I detta syfte ska en klassificering av uppgifter som säkerhetsskyddsklassificerade EU-uppgifter inbegripa en förhandsbedömning av konfidentialitetsnivån och ett beslut från upphovsmannen om att röjande av uppgifterna utan tillstånd skulle kunna vålla unionens eller en eller flera av dess medlemsstaters eller enskilda personers intressen skada i viss grad.

4. När beslutet att säkerhetsskyddsklassificera uppgifterna väl fattats ska detta följas av en andra förhandsbedömning som syftar till att fastställa den lämpliga säkerhetsskyddsklassificeringsnivån. Säkerhetsskyddsklassificeringen av en handling ska avgöras av hur känsligt dess innehåll är.

5. Uteslutande upphovsmannen ska ansvara för att säkerhetsskyddsklassificera uppgifterna. Parlamentets tjänstemän ska säkerhetsskyddsklassificera uppgifter på uppdrag av eller genom delegering från generalsekreteraren.

6. Säkerhetsskyddsklassificering ska utföras korrekt och användas sparsamt. Upphovsmannen till en handling som ska säkerhetsskyddsklassificeras ska undvika varje tendens att placera handlingen på en alltför hög respektive låg säkerhetsskyddsklassificeringsnivå.

7. Den säkerhetsskyddsklassificeringsnivå som ges ska bestämma relevant skyddsnivå när det gäller personlig säkerhet, fysisk säkerhet, administrativ säkerhet och informationssäkring.

8. Uppgifter som motiverar säkerhetsskyddsklassificering ska markeras och hanteras som sådana, oberoende av deras fysiska form. Säkerhetsskyddsklassificeringen ska klart och tydligt meddelas mottagarna, antingen genom säkerhetsskyddsklassificeringsmarkering (om den levereras skriftligen, t.ex. på papper eller inom ett kommunikations- och informationssystem) eller genom ett annat tillkännagivande (om den levereras muntligen, t.ex. under ett samtal eller ett sammanträde inom stängda dörrar). Säkerhetsskyddsklassificerat material ska bära en fysisk markering så att dess säkerhetsskyddsklassificering är lätt identifierbar.

9. Säkerhetsskyddsklassificerade EU-uppgifter i elektronisk form får endast framställas inom ett ackrediterat kommunikations- och informationssystem. De säkerhetsskyddsklassificerade EU-uppgifterna i sig samt filnamnet och lagringsenheten (om extern, t.ex. en cd-skiva eller ett USB-minne) ska bära den relevanta säkerhetsskyddsklassificeringsmarkeringen.

10. Uppgifterna ska säkerhetsskyddsklassificeras så snart de framställs. Exempelvis ska personliga anteckningar, utkast eller e-postmeddelanden som innehåller uppgifter som motiverar säkerhetsskyddsklassificering markeras som säkerhetsskyddsklassificerade EU-uppgifter redan från början, och de ska sammanställas och hanteras i enlighet med detta beslut och dess hanteringsanvisningar i termer av den fysiska och tekniska hanteringen. Sådana uppgifter kan därefter utvecklas till en officiell handling som i sin tur ges en passande markering och hantering. Under utarbetandeprocessen kan en officiell handling behöva bli föremål för en ny utvärdering och ges en högre eller lägre säkerhetsskyddsklassificering beroende på utvecklingen.

11. Upphovsmannen kan besluta sig för att tilldela uppgiftskategorier som han eller hon framställer regelbundet en standardsäkerhetsskyddsklassificering. Vederbörande ska emellertid i detta sammanhang se till att enskilda uppgifter inte systematiskt placeras på en alltför hög respektive låg säkerhetsskyddsklassificeringsnivå.

12. Säkerhetsskyddsklassificerade EU-uppgifter ska alltid bära en säkerhetsskyddsklassificeringsmarkering som motsvarar deras säkerhetsskyddsklassificeringsnivå.

B.1. ***Säkerhetsskyddsklassificeringsnivåer***

13. Säkerhetsskyddsklassificerade EU-uppgifter ska placeras på följande säkerhetsskyddsklassificeringsnivåer:

— TRÈS SECRET UE/EU TOP SECRET, enligt definitionen i artikel 2 d i detta beslut, för uppgifter vars röjande sannolikt skulle

a) utgöra ett direkt hot mot unionens eller en eller flera av dess medlemsstaters inre stabilitet eller mot tredjestater eller internationella organisationer,

b) vålla synnerligen allvarlig skada på förbindelserna med tredjestater eller internationella organisationer,

c) leda direkt till omfattande förlust av liv,

d) vålla synnerligen allvarlig skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters utstationerade personal eller på den fortsatta effektiviteten i ytterst värdefulla säkerhets- eller underrättelseoperationer,

e) vålla allvarlig långsiktig skada på unionens eller medlemsstaternas ekonomier.

— SECRET UE/EU SECRET, enligt definitionen i artikel 2 d i detta beslut, för uppgifter vars röjande sannolikt skulle

a) skapa internationella spänningar i betydande utsträckning,

b) allvarligt skada förbindelserna med tredjestater och internationella organisationer,

c) utgöra ett direkt hot mot liv eller allvarligt skada den allmänna ordningen eller den enskildes säkerhet eller frihet,

d) skada viktiga affärsmässiga eller politiska förhandlingar och därigenom skapa betydande operativa problem för unionen eller för medlemsstaterna,

e) vålla allvarlig skada på den operativa säkerheten i medlemsstaterna eller på effektiviteten i ytterst värdefulla säkerhets- eller underrättelseoperationer,

f) vålla väsentlig materiell skada på unionens eller medlemsstaternas finansiella, monetära, ekonomiska och kommersiella intressen,

g) väsentligt undergräva större organisationers eller aktörers finansiella livskraft,

h) allvarligt hindra utvecklingen eller genomförandet av unionens strategier med stora ekonomiska, handelsrelaterade eller finansiella konsekvenser.

— CONFIDENTIEL UE/EU CONFIDENTIAL, enligt definitionen i artikel 2 d i detta beslut, för uppgifter vars röjande sannolikt skulle

a) skada diplomatiska förbindelser i betydande utsträckning, t.ex. förorsaka formella protester eller andra sanktioner,

b) utgöra ett hot mot den enskildes säkerhet eller frihet,

c) utgöra ett allvarligt hot mot affärsmässiga eller politiska förhandlingar och därigenom skapa operativa problem för unionen eller en eller flera av medlemsstaterna,

d) vålla skada på den operativa säkerheten i en eller flera av medlemsstaterna eller på effektiviteten i säkerhets- eller underrättelseoperationer,

e) väsentligt undergräva större organisationers eller aktörers finansiella livskraft,

f) hindra utredning eller underlätta bedrivande av brottslig verksamhet eller terroristverksamhet,

g) väsentligt motarbeta unionens eller medlemsstaternas finansiella, monetära, ekonomiska och kommersiella intressen, eller

h) allvarligt hindra utvecklingen eller genomförandet av EU:s strategier med stora ekonomiska, handelsrelaterade eller finansiella konsekvenser.

— RESTREINT UE/EU RESTRICTED, enligt definitionen i artikel 2 d i detta beslut, för uppgifter vars röjande sannolikt skulle

a) vara till nackdel för EU:s allmänna intressen,

b) påverka diplomatiska förbindelser negativt,

c) vålla väsentligt obehag för enskilda personer eller företag,

d) vara till nackdel för unionen eller medlemsstaterna inom ramen för affärsmässiga eller politiska förhandlingar,

e) göra det svårare att upprätthålla en effektiv säkerhet inom unionen eller i medlemsstaterna,

f) hindra en effektiv utveckling eller ett effektivt genomförande av unionens strategier,

g) undergräva en god förvaltning av unionen och dess uppdrag,

h) bryta mot parlamentets åtaganden att upprätthålla säkerhetsskyddsklassificeringen för uppgifter som tillhandahålls av tredje part,

i) bryta mot lagstadgade restriktioner om utlämnande av uppgifter,

j) vålla finansiell förlust eller underlätta otillbörlig vinning eller fördel för enskilda personer eller företag, eller

k) skada brottsutredningar eller göra det lättare att begå brott.

B.2. ***Säkerhetsskyddsklassificering av sammanställningar, omslag och utdrag***

14. En skrivelse eller en not som åtföljs av bilagor ska placeras på samma säkerhetsskyddsklassificeringsnivå som den högsta säkerhetsskyddsklassificeringsnivå som tilldelats en av bilagorna. Upphovsmannen ska tydligt ange med vilken säkerhetsskyddsklassificeringsnivå skrivelsen eller noten ska förses när den skilts från de bifogade handlingarna. Om omslagsnoten/skrivelsen inte behöver säkerhetsskyddsklassificeras ska den innehålla följande avslutande formulering: ”Denna not/skrivelse ska inte vara säkerhetsskyddsklassificerad när den skilts från de bifogade handlingarna.”

15. Handlingar eller datafiler som innehåller delar på olika säkerhetsskyddsklassificeringsnivåer ska närhelst detta är möjligt struktureras så att delar på olika säkerhetsskyddsklassificeringsnivå vid behov lätt kan identifieras och avskiljas. Den övergripande säkerhetsskyddsklassificeringsnivån för en handling eller en datafil ska vara minst lika hög som den del som fått den högsta säkerhetsskyddsklassificeringsnivån.

16 Enstaka sidor, stycken, avsnitt, bilagor, tillägg och bifogade ark till en viss handling kan kräva placering på olika säkerhetsskyddsklassificeringsnivåer och ska säkerhetsskyddsklassificeras i enlighet med detta. Standardförkortningar får användas i handlingar som innehåller säkerhetsskyddsklassificerade EU-uppgifter för att ange säkerhetsskyddsklassificeringsnivån för avsnitt eller textstycken vars storlek är mindre än en sida.

17. När uppgifter från olika källor sammanställs ska den slutliga produkten ses över för att dess övergripande säkerhetsskyddsklassificeringsnivå ska kunna fastställas, eftersom den kan motivera en högre säkerhetsskyddsklassificeringsnivå än säkerhetsskyddsklassificeringsnivån för de enskilda delarna.

C. **ANDRA SEKRETESSBELAGDA UPPGIFTER**

18. ”Andra sekretessbelagda uppgifter” ska markeras i enlighet med avsnitt E i detta säkerhetsmeddelande samt hanteringsanvisningarna.

D. **FRAMSTÄLLANDE AV SEKRETESSBELAGDA UPPGIFTER**

19. Endast personer som är vederbörligen behöriga på grundval av detta beslut eller tillstånd från säkerhetsmyndigheten får framställa sekretessbelagda uppgifter.

20. Sekretessbelagda uppgifter ska inte inkluderas i internet- eller intranätbaserade system för dokumenthantering.

D.1. ***Framställande av säkerhetsskyddsklassificerade EU-uppgifter***

21. För att framställa säkerhetsskyddsklassificerade EU-uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET ska den berörda personen vara behörig enligt detta beslut eller ska först ha fått tillstånd enligt artikel 4.1 i detta beslut.

22. Säkerhetsskyddsklassificerade EU-uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET ska framställas endast inom det säkra området.

23. Följande bestämmelser ska tillämpas vid framställande av säkerhetsskyddsklassificerade EU-uppgifter:

a) Varje sida ska tydligt märkas med den tillämpliga säkerhetsskyddsklassificeringsnivån.

b) Varje sida ska vara numrerad och ska ange det totala antalet sidor.

c) Handlingen ska bära ett referensnummer på första sidan och en angivelse av ämnet, som i sig inte ska utgöra säkerhetsskyddsklassificerade uppgifter, om det inte fastsatts som sådana.

d) Handlingens första sida ska förses med datum.

e) Första sidan i varje handling som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET ska innehålla en förteckning över alla bilagor och bifogade ark.

f) Handlingar som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET ska ha ett exemplarnummer på varje sida, om de ska sändas ut i flera exemplar. Varje exemplar ska också på första sidan ha en angivelse av det totala antalet exemplar och sidor.

g) Om handlingen innehåller hänvisningar till andra handlingar som innehåller säkerhetsskyddsklassificerade uppgifter från andra unionsinstitutioner, eller om den innehåller säkerhetsskyddsklassificerade uppgifter som har sitt ursprung i sådana handlingar, ska den placeras på samma säkerhetsskyddsklassificeringsnivå som de handlingarna placerats på, och handlingen i fråga får inte utan skriftligt samtycke från upphovsmannen spridas till andra personer än dem som ingår i sändlistan när det gäller den ursprungliga handlingen eller andra handlingar som innehåller säkerhetsskyddsklassificerade uppgifter.

24. Upphovsmannen ska behålla kontrollen över de säkerhetsskyddsklassificerade EU-uppgifter som denne har framställt. Hans eller hennes skriftliga samtycke ska sökas innan säkerhetsskyddsklassificerade EU-uppgifter

a) placeras på en lägre säkerhetsskyddsklassificeringsnivå eller blir föremål för ett beslut om att de inte längre ska vara säkerhetsskyddsklassificerade,

b) används för andra ändamål än dem som fastställts av upphovsmannen,

c) lämnas ut till tredjestat eller internationell organisation,

d) lämnas ut till andra personer, institutioner, länder eller internationella organisationer än de adressater som upphovsmannen ursprungligen gav tillstånd för när det gäller att konsultera uppgifterna i fråga,

e) lämnas ut till en uppdragstagare eller presumtiv uppdragstagare i en tredjestat,

f) kopieras eller översätts, om uppgifterna placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET,

g) destrueras.

D.2. ***Framställande av andra sekretessbelagda uppgifter***

25. Generalsekreteraren får i egenskap av säkerhetsmyndighet besluta huruvida tillstånd att framställa ”andra sekretessbelagda uppgifter” ska beviljas en viss funktion, avdelning och/eller person.

26. ”Andra sekretessbelagda uppgifter” ska markeras på ett av de sätt som fastställs i hanteringsanvisningarna.

27. Följande bestämmelser ska tillämpas vid framställande av ”andra sekretessbelagda uppgifter”:

a) Deras markering ska anges överst på handlingens första sida.

b) Varje sida ska vara numrerad, med angivande även av det totala antalet sidor.

c) Handlingen ska bära ett referensnummer på första sidan och en angivelse av ämnet.

d) Handlingens första sida ska förses med datum.

e) Handlingens sista sida ska innehålla en förteckning över alla bilagor och bifogade ark.

28. Framställande av ”andra sekretessbelagda uppgifter” ska omfattas av särskilda bestämmelser och förfaranden som fastställs i hanteringsanvisningarna.

E. **SÄKERHETSBETECKNINGAR OCH MARKERINGAR**

29. Säkerhetsbeteckningar och markeringar på handlingar är avsedda att kontrollera uppgiftsflödet och begränsa tillgången till sekretessbelagda uppgifter på grundval av principen om behov av kännedom i tjänsten.

30. När säkerhetsbeteckningar och/eller markeringar används eller fastsätts ska det göras med försiktighet så att det inte sker någon sammanblandning med säkerhetsskyddsklassificeringarna för säkerhetsskyddsklassificerade EU-uppgifter: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET.

31. Särskilda bestämmelser om användning av säkerhetsbeteckningar och markeringar ska, tillsammans med förteckningen över Europaparlamentets godkända säkerhetsbeteckningar, fastställas i hanteringsanvisningarna.

E.1. ***Säkerhetsbeteckningar***

32. Säkerhetsbeteckningar får endast användas tillsammans med en säkerhetsskyddsklassificering och ska inte tillämpas separat på handlingar. En säkerhetsbeteckning får tillämpas på säkerhetsskyddsklassificerade EU-uppgifter för att

a) begränsa en säkerhetsskyddsklassificerings giltighet (för säkerhetsskyddsklassificerade uppgifter som innebär en automatisk placering på en lägre säkerhetsskyddsklassificeringsnivå eller att uppgifter inte längre ska vara säkerhetsskyddsklassificerade),

b) begränsa utlämnandet av de säkerhetsskyddsklassificerade EU-uppgifterna i fråga,

c) fastställa särskilda hanteringsarrangemang utöver vad som framgår av säkerhetsskyddsklassificeringsnivån.

33. De extra kontroller som är tillämpliga på hantering och lagring av handlingar som innehåller säkerhetsskyddsklassificerade EU-uppgifter medför ytterligare bördor för alla involverade parter. För att minimera det arbete som krävs i detta sammanhang är det god praxis att, när sådana handlingar framställs, fastställa en tidsfrist eller händelse efter vilken säkerhetsskyddsklassificeringen automatiskt ska löpa ut och de uppgifter som ingår i handlingen ska placeras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade.

34. Om en handling berör ett specifikt arbetsområde och dess utlämnande måste begränsas och/eller den ska bli föremål för särskilda hanteringsarrangemang kan ett motsvarande meddelande bifogas säkerhetsskyddsklassificeringen för att bidra till att identifiera målgruppen.

E.2. ***Markeringar***

35. Markeringar ska inte utgöra en säkerhetsskyddsklassificering. De är avsedda att endast tillhandahålla konkreta anvisningar om hanteringen av en handling och ska inte användas för att beskriva innehållet i en sådan handling.

36. Markeringar får tillämpas separat på handlingar eller användas tillsammans med en säkerhetsskyddsklassificering.

37. Som en generell regel ska markeringar tillämpas på uppgifter som omfattas av tystnadsplikt (som avses i artikel 339 i EUF-fördraget och artikel 17 tjänsteföreskrifterna; eller som parlamentet måste skydda av juridiska skäl), medan uppgifterna i fråga inte behöver (eller inte kan) säkerhetsskyddsklassificeras.

E.3. ***Användning av markeringar i kommunikationssystem- och informationssystemen***

38. Bestämmelserna om användning av markeringar ska också vara tillämpliga i de ackrediterade kommunikationssystem- och informationssystemen.

39. Ackrediteringsmyndigheten för säkerhet ska fastställa särskilda bestämmelser om användning av markeringar i de ackrediterade kommunikationssystem- och informationssystemen.

F. **MOTTAGANDE AV UPPGIFTER**

40. Endast enheten för sekretessbelagda uppgifter ska vara behörig inom parlamentet att ta emot uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET och högre eller motsvarande från tredje part.

41. När det gäller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” får både enheten för sekretessbelagda uppgifter och den behöriga instansen/befattningshavaren inom parlamentet ansvara för att ta emot uppgifterna från tredje part, och för att tillämpa de principer som anges i detta säkerhetsmeddelande.

G. **REGISTRERING**

42. Med registrering avses tillämpning av förfaranden som registrerar de sekretessbelagda uppgifternas livscykel, inbegripet faser som innebär att uppgifterna sprids, konsulteras och destrueras.

43. Vid tillämpningen av detta säkerhetsmeddelande avses med ”diarium” ett register där de datum och klockslag registerförs då sekretessbelagda uppgifter

a) inkommer hos eller lämnar respektive sekretariat för instansen/befattningshavaren inom parlamentet eller, allt efter omständigheterna, enheten för sekretessbelagda uppgifter,

b) konsulteras av eller överlämnas till en person som säkerhetsprövats,

c) destrueras.

44. Upphovsmannen till sekretessbelagda uppgifter ska ansvara för att markera den första förklaringen vid upprättandet av en handling som innehåller sådana uppgifter. Den förklaringen ska meddelas enheten för sekretessbelagda uppgifter när handlingen upprättas.

45. Endast enheten för sekretessbelagda uppgifter får av säkerhetsskäl registrera uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” från tredje part ska av administrativa skäl registreras av den avdelning som ansvarar för det officiella mottagandet av handlingen, dvs. antingen enheten för sekretessbelagda uppgifter eller sekretariatet för instansen/befattningshavaren inom parlamentet. ”Andra sekretessbelagda uppgifter” som framställts inom parlamentet ska av administrativa skäl registreras av upphovsmannen.

46. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska registreras i synnerhet när

a) de framställs,

b) de inkommer hos eller lämnar enheten för sekretessbelagda uppgifter, och

c) de införs i eller lämnar kommunikations- och informationssystemen.

47. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande ska registreras i synnerhet när

a) de framställs,

b) de inkommer hos eller lämnar respektive sekretariat för instansen/befattningshavaren inom parlamentet eller enheten för sekretessbelagda uppgifter,

c) de införs i eller lämnar ett kommunikations- och informationssystem.

48. Registrering av sekretessbelagda uppgifter kan göras i pappersform eller i elektroniska diarier/kommunikations- och informationssystem.

49. För uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” ska åtminstone följande registreras:

a) Det datum och klockslag då uppgifterna inkommer hos eller lämnar respektive sekretariat för instansen/befattningshavaren inom parlamentet eller, allt efter omständigheterna, enheten för sekretessbelagda uppgifter.

b) Handlingens titel, säkerhetsskyddsklassificeringsnivån eller markeringen, det datum då säkerhetsskyddsklassificeringen/markeringen löper ut och eventuella referensnummer som handlingen försetts med.

50. För uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska åtminstone följande registreras:

a) Det datum och klockslag då uppgifterna inkommer hos eller lämnar enheten för sekretessbelagda uppgifter.

b) Handlingens titel, säkerhetsskyddsklassificeringsnivån eller markeringen, eventuella referensnummer som handlingen försetts med och det datum då säkerhetsskyddsklassificeringen/markeringen löper ut.

c) Uppgifter om upphovsmannen.

d) Uppgift om identiteten på den person som har getts tillgång till handlingen och den dag då handlingen konsulterades av den personen.

e) Uppgift om eventuella kopior eller översättningar som gjorts av handlingen.

f) Det datum och klockslag då eventuella kopior eller översättningar av handlingen lämnar eller återlämnas till enheten för sekretessbelagda uppgifter, och uppgifter om vart de har skickats och vem som återlämnat dem.

g) Uppgift om det datum och klockslag då handlingen destruerades, och om vem som destruerade den, i enlighet med parlamentets säkerhetsbestämmelser om destruering.

h) Uppgift om att handlingen inte längre ska vara säkerhetsskyddsklassificerad eller att den ska placeras på en lägre säkerhetsskyddsklassificeringsnivå.

51. Diarier ska säkerhetsskyddsklassificeras eller markeras beroende på vad som är lämpligt. Diarier för uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska registreras på samma nivå.

52. Säkerhetsskyddsklassificerade uppgifter kan registreras

a) i ett enda diarium, eller

b) i separata diarier enligt säkerhetsskyddsklassificeringsnivå, enligt huruvida uppgifterna är inkommande eller utgående och enligt ursprung eller destination.

53. Vid elektronisk hantering inom ett kommunikations- och informationssystem kan registreringsförfarandena göras med processer i själva kommunikations- och informationssystemet som uppfyller krav som är likvärdiga med dem som anges ovan. Närhelst säkerhetsskyddsklassificerade EU-uppgifter lämnar kommunikations- och informationssystemet ska ovan beskrivna registreringsförfaranden tillämpas.

54. Enheten för sekretessbelagda uppgifter ska registerföra alla säkerhetsskyddsklassificerade uppgifter som parlamentet lämnar ut till tredje part och alla säkerhetsskyddsklassificerade uppgifter som parlamentet tar emot från tredje part.

55. När väl registreringen av uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande har slutförts ska enheten för sekretessbelagda uppgifter kontrollera huruvida adressaten har giltig säkerhetsbehörighet. Om behörighet föreligger ska adressaten meddelas av enheten för sekretessbelagda uppgifter. Konsultation av säkerhetsskyddsklassificerade uppgifter får endast äga rum först när den handling som innehåller uppgifterna i fråga registrerats.

H. **DISTRIBUTION**

56. Upphovsmannen ska upprätta en första sändlista för säkerhetsskyddsklassificerade EU-uppgifter som han eller hon har framställt.

57. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED och andra sekretessbelagda uppgifter som parlamentet framställt ska distribueras inom parlamentet av upphovsmannen, i enlighet med de relevanta hanteringsanvisningarna och på grundval av principen om behov av kännedom i tjänsten. För uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET och som framställts av parlamentet inom det säkra området ska sändlistan (och eventuella ytterligare anvisningar i fråga om distribution) tillhandahållas enheten för sekretessbelagda uppgifter, som ska vara ansvarig för förvaltningen av den.

58. Endast enheten för sekretessbelagda uppgifter får distribuera säkerhetsskyddsklassificerade EU-uppgifter som framställts av parlamentet till tredje part, på grundval av principen om behov av kännedom i tjänsten.

59. Sekretessbelagda uppgifter som mottagits av antingen enheten för sekretessbelagda uppgifter eller någon instans/befattningshavare inom parlamentet som inkommit med en sådan begäran ska distribueras i enlighet med mottagna anvisningar från upphovsmannen.

I. **HANTERING, LAGRING OCH KONSULTATION**

60. Hantering, lagring och konsultation av sekretessbelagda uppgifter ska ske i enlighet med säkerhetsmeddelande 4 och hanteringsanvisningarna.

J. **KOPIERING/ÖVERSÄTTNING/TOLKNING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER**

61. Handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET får inte kopieras eller översättas utan föregående skriftligt samtycke från upphovsmannen. Handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller motsvarande eller på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande får kopieras eller översättas på innehavarens begäran under förutsättning att upphovsmannen inte förbjudit detta.

62. Alla kopior av handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET eller CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande ska av säkerhetsskäl registreras.

63. De säkerhetsåtgärder som ska tillämpas på den originalhandling som innehåller säkerhetsskyddsklassificerade uppgifter ska även tillämpas på kopior och översättningar av den.

64. Handlingar som mottas från rådet bör inkomma på alla officiella språk.

65. Kopior och/eller översättningar av handlingar som innehåller säkerhetsskyddsklassificerade uppgifter får begäras av upphovsmannen eller innehavaren av kopior. Kopior av handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande får framställas endast i det säkra området och genom användning av kopiatorer som utgör en del av ett ackrediterat kommunikations- och informationssystem. Kopior av handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och andra sekretessbelagda uppgifter ska göras genom användning av en ackrediterad kopieringsapparat i parlamentets lokaler.

66. Alla kopior och översättningar av handlingar eller delar av kopior av handlingar som innehåller sekretessbelagda uppgifter ska vara vederbörligen markerade, numrerade och registrerade.

67. Det ska inte göras fler kopior än vad som är strikt nödvändigt. Alla kopior ska destrueras i enlighet med hanteringsanvisningarna i slutet av konsultationsperioden.

68. Endast tolkar och översättare som är tjänstemän vid parlamentet ska ges tillgång till säkerhetsskyddsklassificerade uppgifter ska vara tjänstemän vid parlamentet.

69. Tolkar och översättare med tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska ha genomgått lämplig säkerhetsprövning.

70. Tolkar och översättare som arbetar med handlingar som innehåller uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska arbeta i det säkra området.

K. PLACERING PÅ EN LÄGRE SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅ, BESLUT ATT UPPGIFTER INTE LÄNGRE SKA VARA SÄKERHETSSKYDDSKLASSIFICERADE OCH AVMARKERING AV SEKRETESSBELAGDA UPPGIFTER

K.1. *Allmänna principer*

71. Sekretessbelagda uppgifter ska inte längre vara säkerhetsskyddsklassificerade, ska placeras på en lägre säkerhetsskyddsklassificeringsnivå eller ska avmarkeras när skydd inte längre behövs eller inte längre behövs på den ursprungliga nivån.

72. Beslut om att placera uppgifter på en lägre säkerhetsskyddsklassificeringsnivå, att uppgifter inte längre ska vara säkerhetsskyddsklassificerade och att avmarkera uppgifter som ingår i handlingar som upprättats av parlamentet kan även behöva fattas från fall till fall, t.ex. med anledning av en begäran om tillgång från allmänheten eller från en annan EU-institution, eller på initiativ av enheten för sekretessbelagda uppgifter eller en behörig instans/befattningshavare inom parlamentet.

73. Vid tidpunkten för framställandet ska upphovsmannen till säkerhetsskyddsklassificerade EU-uppgifter, där så är möjligt, ange om de säkerhetsskyddsklassificerade EU-uppgifterna kan placeras på en lägre säkerhetsskyddsklassificeringsnivå, eller om det kan beslutas att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade från ett visst datum eller efter en särskild händelse. När det inte är praktiskt möjligt att lämna en sådan uppgift ska upphovsmannen, enheten för sekretessbelagda uppgifter eller den instans/befattningshavare inom parlamentet som innehar uppgifterna se över säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifterna åtminstone vart femte år. Säkerhetsskyddsklassificerade EU-uppgifter får under alla omständigheter placeras på en lägre säkerhetsskyddsklassificeringsnivå eller beslutas inte längre vara säkerhetsskyddsklassificerade endast med skriftligt förhandssamtycke från upphovsmannen.

74. Om upphovsmannen till säkerhetsskyddsklassificerade EU-uppgifter inte kan fastställas eller spåras när det gäller handlingar som upprättats inom parlamentet ska säkerhetsmyndigheten se över säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifterna på förslag av den instans/befattningshavare inom parlamentet som innehar uppgifterna, vilken kan samråda med enheten för sekretessbelagda uppgifter i detta avseende.

75. Enheten för sekretessbelagda uppgifter eller den instans/befattningshavare inom parlamentet som innehar uppgifterna ska vara ansvariga för att informera mottagaren eller mottagarna om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade eller att uppgifterna placerats på en lägre säkerhetsskyddsklassificeringsnivå, och adressaterna ska i sin tur vara ansvariga för att informera eventuella efterföljande mottagare till vilka de har översänt handlingen eller kopior av handlingen.

76. Beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade, placering på en lägre säkerhetsskyddsklassificeringsnivå och avmarkering av uppgifter som ingår i en handling ska registreras.

K.2. *Beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade*

77. Säkerhetsskyddsklassificerade EU-uppgifter får helt eller delvis beslutas inte längre vara säkerhetsskyddsklassificerade. De får delvis beslutas inte längre vara säkerhetsskyddsklassificerade om skyddet inte längre bedöms vara nödvändigt för en viss del av den handling som innehåller uppgifterna men bedöms vara motiverat för handlingens resterande delar.

78. Om översynen av säkerhetsskyddsklassificerade EU-uppgifter som ingår i en handling som upprättats inom parlamentet resulterar i ett beslut att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade ska hänsyn tas till huruvida handlingen får offentliggöras eller huruvida den ska förses med en distributionsmarkering (dvs. inte offentliggöras).

79. När det fattas beslut om att säkerhetsskyddsklassificerade EU-uppgifter inte längre ska vara säkerhetsskyddsklassificerade ska detta registreras i diariet med följande uppgifter: datum för beslutet om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade, namnet på de personer som begärde detta och de personer som godkände det, referensnummer på den handling om vilken beslut fattats om att den inte längre ska vara säkerhetsskyddsklassificerad samt handlingens slutdestination.

80. De gamla säkerhetsskyddsklassificeringsmarkeringarna i den handling om vilken beslut fattats om att den inte längre ska vara säkerhetsskyddsklassificerad samt i alla kopior av denna måste strykas över. Handlingarna och alla kopior av dem ska lagras i enlighet med detta.

81. Vid beslut om att säkerhetsskyddsklassificerade uppgifter delvis inte längre ska vara säkerhetsskyddsklassificerade ska den del om vilken beslut fattats om att den inte längre ska vara säkerhetsskyddsklassificerad upprättas i form av ett utdrag och lagras i enlighet med detta. Den behöriga avdelningen ska registerföra

a) datumet för beslutet om att uppgifter delvis inte längre ska vara säkerhetsskyddsklassificerade,

b) namnen på både de personer som begärde detta och de personer som godkände det,

c) referensnumret på det utdrag om vilket beslut fattats om att det inte längre ska vara säkerhetsskyddsklassificerat.

K.3. ***Placering på en lägre säkerhetsskyddsklassificeringsnivå***

82. Efter placeringen av säkerhetsskyddsklassificerade uppgifter på en lägre säkerhetsskyddsklassificeringsnivå ska den handling där de återfinns registreras i diarierna, enligt såväl den gamla som den nya nivån. Datumet för placering på en lägre säkerhetsskyddsklassificeringsnivå ska registreras, liksom namnet på den person som godkänt detta.

83. Den handling som innehåller uppgifter som placerats på en lägre säkerhetsskyddsklassificeringsnivå och alla kopior av den ska säkerhetsskyddsklassificeras med den nya säkerhetsskyddsklassificeringsnivån och lagras i enlighet med detta.

L. **DESTRUERING AV SEKRETESSBELAGDA UPPGIFTER**

84. Sekretessbelagda uppgifter (i pappersform eller i elektronisk form) som inte längre behövs ska destrueras eller raderas, i enlighet med hanteringsanvisningarna och relevanta bestämmelser om arkivering.

85. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller UE/EU SECRET eller motsvarande ska destrueras av enheten för sekretessbelagda uppgifter. Destrueringen ska ske i närvaro av en person som genomgått säkerhetsprövning motsvarande åtminstone säkerhetsskyddsklassificeringsnivån för de uppgifter som destrueras.

86. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande får destrueras endast med skriftligt förhandssamtycke från upphovsmannen.

87. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska destrueras och undanskaffas av enheten för sekretessbelagda uppgifter på begäran av upphovsmannen eller en behörig myndighet. Diarierna och andra register ska uppdateras i enlighet med detta. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande ska destrueras och undanskaffas av antingen enheten för sekretessbelagda uppgifter eller den berörda instansen/befattningshavaren inom parlamentet.

88. Den tjänsteman som ansvarar för destrueringen samt den person som närvarar vid destrueringen ska underteckna ett destrueringsintyg som ska inregistreras och arkiveras hos enheten för sekretessbelagda uppgifter. Enheten för sekretessbelagda uppgifter ska, tillsammans med sändlistorna, i minst tio år bevara destrueringsintygen för uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande och i minst fem år bevara destrueringsintygen för uppgifter som placerats på säkerhetsskyddsklassificeringsnivån SECRET UE/EU TOP SECRET eller motsvarande eller säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller motsvarande.

89. Handlingar som innehåller säkerhetsskyddsklassificerade uppgifter ska destrueras enligt metoder som uppfyller relevanta EU-standarder eller likvärdiga standarder för att hindra fullständig eller partiell rekonstruktion.

90. Destruering av lagringsmedier för datorer som använts för säkerhetsskyddsklassificerade uppgifter ska ske i enlighet med de relevanta hanteringsanvisningarna.

91. Destruering av säkerhetsskyddsklassificerade uppgifter ska registreras i det relevanta diariet med följande uppgifter:

a) Datum och klockslag för destruering.

b) Namnet på den tjänsteman som ansvarade för destrueringen.

c) Identifiering av den handling eller de kopior som destruerats.

d) Den ursprungliga fysiska formen för de destruerade säkerhetsskyddsklassificerade EU-uppgifterna.

e) Destrueringsmetoden.

f) Platsen för destruering.

M. **ARKIVERING**

92. Säkerhetsskyddsklassificerade uppgifter, inklusive omslagsnot/skrivelse, bilagor, inlämningskvitto och/eller andra delar av ärendemappen, ska överföras till det säkra arkivet i det säkra området sex månader efter det att de senast konsulterades och senast ett år efter det att de lämnades in. Närmare bestämmelser om arkivering av säkerhetsskyddsklassificerade uppgifter ska fastställas i hanteringsanvisningarna.

93. För ”andra sekretessbelagda uppgifter” ska de allmänna bestämmelserna om dokumenthantering tillämpas utan att det påverkar eventuella andra specifika bestämmelser om hantering av sådana uppgifter.

SÄKERHETSMEDDELANDE 3

BEHANDLING AV SEKRETESSBELAGDA UPPGIFTER MED HJÄLP AV AUTOMATISERADE KOMMUNIKATIONS- OCH INFORMATIONS-SYSTEM

A. **INFORMATIONSSÄKRING AV SÄKERHETSSKYDDS-KLASSIFICERADE UPPGIFTER SOM HANTERAS I INFORMATIONSSYSTEM**

1. Med informationssäkring på området informationssystem avses förvissningar om att dessa system kommer att skydda de säkerhetsskyddsklassificerade uppgifter de hanterar och kommer att fungera som de ska, och när det krävs, under kontroll av behöriga användare. Effektiv informationssäkring ska garantera lämpliga nivåer för konfidentialitet, riktighet, tillgänglighet, oavvislighet och autenticitet. Informationssäkring ska grundas på en riskhanteringsprocess.

2. Med kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade uppgifter avses ett system som gör det möjligt att hantera information i elektronisk form. Ett sådant informationssystem ska innefatta alla de resurser som krävs för att det ska fungera, inklusive infrastruktur, organisation, personal och informationsresurser.

3. Detta kommunikations- och informationssystem ska hantera säkerhetsskyddsklassificerade uppgifter i enlighet med informationssäkringsbegreppet.

4. Kommunikations- och informationssystem ska genomgå en ackrediteringsprocess. Ackrediteringen ska syfta till att skapa förvissning om att alla lämpliga säkerhetsåtgärder har vidtagits och att tillräckligt hög skyddsnivå för de säkerhetsskyddsklassificerade uppgifterna och för systemen har uppnåtts i enlighet med detta säkerhetsmeddelande. I redovisningen av ackrediteringen ska fastställas högsta säkerhetsskyddsklassificeringsnivå för de uppgifter som får hanteras av systemen och motsvarande villkor.

5. Följande egenskaper och koncept för informationssäkring är av största betydelse för säkerheten och för att driften av kommunikations- och informationssystem ska kunna fungera på ett korrekt sätt:

a) Autenticitet: garanti för att uppgifterna är riktiga och att de härrör från angivna källor.

b) Tillgänglighet: egenskapen att finnas tillgänglig och vara användbar på begäran för en behörig enhet.

c) Konfidentialitet: egenskapen att uppgifter inte kommer att röjas för obehöriga personer, enheter eller processer.

d) Riktighet: egenskapen att skydda uppgifternas och tillgångarnas exakthet och fullständighet.

e) Oavvislighet: möjligheten att bevisa att en åtgärd eller händelse har ägt rum, för att utesluta möjligheten att denna händelse eller åtgärd senare förnekas.

B. **PRINCIPER FÖR INFORMATIONSSÄKRING**

6. De bestämmelser som anges nedan ska utgöra grunden för säkerheten för alla kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter. Detaljerade krav för genomförandet av dessa bestämmelser ska definieras i säkerhetsstrategier och säkerhetsriktlinjer för informationssäkring.

B.1. ***Hantering av säkerhetsrisker***

7. Hantering av säkerhetsrisker ska utgöra en integrerande del av definiering, utveckling, drift och underhåll av systemet. Riskhanteringen (bedömning, hantering, acceptans och kommunikation) ska gemensamt genomföras som en fortlöpande process av företrädare för systemägare, projektmyndigheter, driftsmyndigheter och säkerhetsgodkännande myndigheter enligt säkerhetsmeddelande 1 genom att en beprövad, öppen och begriplig riskbedömningsprocess används. Omfattningen av kommunikations- och informationssystemet och dess tillgångar ska klart definieras när riskhanteringsprocessen inleds.

8. De behöriga myndigheter som fastställs i säkerhetsmeddelande 1 ska se över potentiella hot mot systemet och kontinuerligt göra uppdaterade och noggranna hotbedömningar som avspeglar den befintliga driftsmiljön. De ska kontinuerligt uppdatera sina kunskaper om sårbarhetsfrågor och regelbundet se över sårbarhetsbedömningen för att hålla sig à jour med den föränderliga miljön på it-området.

9. Syftet med säkerhetsriskhantering ska vara att tillämpa en serie säkerhetsåtgärder som resulterar i en tillfredsställande kompromiss mellan användarkrav, kostnader och kvarstående säkerhetsrisker.

10. Ackreditering av ett kommunikations- och informationssystem ska inbegripa en formell redovisning av kvarstående risker och den ansvariga myndighetens acceptans av den kvarstående risken. De särskilda krav, den skala och den grad av detalj som fastställs av den relevanta ackrediteringsmyndigheten för ackreditering av ett kommunikations- och informationssystem ska stå i proportion till den uppskattade risken, med beaktande av alla relevanta faktorer, inklusive säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade uppgifter som hanteras i kommunikations- och informationssystemet.

B.2. ***Säkerhet under kommunikations- och informationssystemets hela livscykel***

11. Att garantera säkerheten ska vara ett krav under kommunikations- och informationssystemets hela livscykel, från inledandet till avvecklingen av systemet.

12. Varje inblandad aktörs roll i och interaktion med systemet när det gäller dess säkerhet ska fastställas för varje skede av livscykeln.

13. Kommunikations- och informationssystemet, inbegripet dess tekniska och icke-tekniska säkerhetsåtgärder, ska säkerhetstestas under ackrediteringsprocessen för att säkerställa att rätt säkringsnivå erhålls och för att kontrollera att kommunikations- och informationssystemet, inbegripet dess tekniska och icke-tekniska säkerhetsåtgärder, är korrekt genomförda, integrerade och konfigurerade.

14. Utvärderingar, inspektioner och översyner av säkerheten ska regelbundet genomföras under systemets drift och underhåll och när exceptionella omständigheter uppkommer.

15. Systemets säkerhetsdokumentering ska utvecklas under dess livscykel såsom en integrerande del av processen för hantering av ändringar.

16. De registreringsförfaranden som vid behov utförs av ett kommunikations- och informationssystem ska kontrolleras som en del av ackrediteringsprocessen.

B.3. ***Bästa praxis***

17. Myndigheten för informationssäkring ska ta fram bästa praxis för skydd av säkerhetsskyddsklassificerade uppgifter som hanteras av systemet. Riktlinjer för bästa praxis ska ange tekniska, fysiska, organisatoriska och förfarandemässiga säkerhetsåtgärder för system vilkas ändamålsenlighet för att motverka givna hot och sårbarheter har bevisats.

18. Vid skyddet av säkerhetsskyddsklassificerade uppgifter som hanteras i systemet ska man utnyttja erfarenheterna vid de enheter som deltar i informationssäkring.

19. Spridningen och det efterföljande genomförandet av bästa praxis ska bidra till uppnåendet av en likvärdig säkerhetsnivå för de system som används av parlamentets generalsekretariat i vilka säkerhetsskyddsklassificerade uppgifter hanteras.

B.4. ***Säkerhet på djupet***

20. För att minska risken i samband med kommunikations- och informationssystemen ska det genomföras en rad tekniska och icke-tekniska säkerhetsåtgärder, organiserade som flera försvarsnivåer. Dessa nivåer ska omfatta följande:

a) Avskräckning: säkerhetsåtgärder vars syfte är att avstyra eventuella fientliga planer på att angripa systemet.

b) Förebyggande: säkerhetsåtgärder vars syfte är att hindra eller blockera ett angrepp mot systemet.

c) Upptäckt: säkerhetsåtgärder vars syfte är att upptäcka ett angrepp mot systemet.

d) Uthållighet: säkerhetsåtgärder vars syfte är att begränsa följderna av ett angrepp till ett minimalt antal uppgifter eller systemtillgångar och att förhindra ytterligare skada.

e) Återställande: säkerhetsåtgärder vars syfte är att återställa en säker situation för systemet.

Hur stränga dessa säkerhetsåtgärder ska vara ska bestämmas genom en riskbedömning.

21. De behöriga myndigheter som anges i säkerhetsmeddelande 1 ska se till att de kan bemöta incidenter som kan gå utöver organisatoriska gränser för att samordna motåtgärder och utbyta information om dessa incidenter och riskerna i samband med dessa (it-baserad kapacitet för incidenthantering).

B.5. ***Principen om minimalitet och begränsad behörighet***

22. För att undvika onödiga risker ska endast väsentliga funktioner, apparater och tjänster som behövs för att uppfylla driftskraven utnyttjas.

23. Användarna av kommunikations- och informationssystem och automatiserade processer ska endast ges det tillträde, de privilegier eller den behörighet de behöver för att utföra sina uppgifter, för att begränsa eventuella skador genom olyckor, misstag eller obehörig användning av systemresurser.

B.6. ***Medvetenhet om informationssäkring***

24. Riskmedvetenhet och tillgängliga skyddsåtgärder utgör den första försvarslinjen för informations- och kommunikationssystemens säkerhet. All personal som är involverad i ett systems livscykel, även användare, ska särskilt inse

a) att säkerhetshaverier kan förorsaka betydande skada i systemen för hantering av säkerhetsskyddsklassificerade uppgifter,

b) den potentiella skada som kan uppstå för andra genom sammankoppling och ett ömsesidigt beroende, och

c) sitt individuella ansvar och sin ansvarsskyldighet för kommunikations- och informationssystemens säkerhet i enlighet med det personliga uppdraget inom systemen och processerna.

25. För att garantera denna insikt om ansvaret för säkerheten ska utbildning i informationssäkring och medvetenhet vara obligatorisk för all inblandad personal, inbegripet den högre ledningen, ledamöter av Europaparlamentet och systemanvändare.

B.7. ***Utvärdering och godkännande av produkter för it-säkerhet***

26. System som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska skyddas på sådant sätt att uppgifterna inte kan läcka ut genom oavsiktlig elektromagnetisk strålning (tempestsäkerhetsåtgärder).

27. Om skyddet av säkerhetsskyddsklassificerade uppgifter tillhandahålls genom kryptoprodukter ska dessa produkter certifieras av ackrediteringsmyndigheten för säkerhet såsom en del av de EU-godkända kryptoprodukterna.

28. När säkerhetsskyddsklassificerade uppgifter överförs på elektronisk väg, ska EU-godkända kryptoprodukter användas. Trots detta krav får specifika förfaranden eller specifika tekniska konfigurationer tillämpas i krissituationer enligt punkterna 41–44.

29. Den erforderliga graden av förtroende i säkerhetsåtgärderna, definierad som en säkringsnivå, ska fastställas i enlighet med resultaten av riskhanteringsprocessen och i linje med relevanta säkerhetsstrategier och säkerhetsriktlinjer.

30. Säkerhetsnivån ska kontrolleras genom att internationellt erkända eller nationellt godkända processer och metoder används. Detta inbegriper i första hand utvärdering, skyddsåtgärder och revision.

31. Ackrediteringsmyndigheten för säkerhet ska godkänna säkerhetsriktlinjer för kvalificering och godkännande av sådana produkter för it-säkerhet som inte används för kryptering.

B.8. ***Överföring inom det säkra området***

32. När överföringen av säkerhetsskyddsklassificerade uppgifter är begränsad till det säkra området får okrypterad distribution eller kryptering på en lägre nivå användas på grundval av resultatet av riskhanteringsförfarandet och med godkännande från ackrediteringsmyndigheten för säkerhet.

B.9. ***Säker sammankoppling mellan kommunikations- och informationssystem***

33. Med sammankoppling avses en direkt förbindelse mellan två eller flera it-system i syfte att utbyta uppgifter och andra informationstillgångar i form av envägs- eller flervägskommunikation.

34. Enheten för sekretessbelagda uppgifter ska behandla alla sammankopplade it-system som icke-tillförlitliga och skyddsåtgärder ska införas för att kontrollera utbytet av säkerhetsskyddsklassificerade uppgifter med andra kommunikations- och informationssystem.

35. För all sammankoppling av kommunikations- och informationssystem med ett annat it-system ska följande grundläggande krav uppfyllas:

a) Verksamhetskrav eller driftskrav för sådan sammankoppling ska fastställas och godkännas av de behöriga myndigheterna.

b) Sammankopplingen i fråga ska genomgå en riskhanterings- och ackrediteringsprocess och ska kräva tillstånd från den behöriga ackrediteringsmyndigheten för säkerhet.

c) Skyddstjänster ska genomföras vid den yttre säkerhetsgränsen för systemen.

36. Det får inte förekomma samtrafik mellan ett ackrediterat kommunikations- och informationssystem och ett oskyddat eller allmänt nät, utom när systemet har godkända skyddstjänster installerade för ett sådant ändamål mellan systemet och det oskyddade eller allmänna nätet. Säkerhetsåtgärderna för sådan samtrafik ska ses över av den behöriga myndigheten för informationssäkring och godkännas av den behöriga ackrediteringsmyndigheten för säkerhet.

37. När det oskyddade eller allmänna nätet används enbart som nätoperatör och data är krypterade med en EU-kryptoprodukt som certifierats i enlighet med punkt 27 ska en sådan sammankoppling inte betraktas som samtrafik.

38. Direkt sammankoppling eller kaskadsammankoppling till ett oskyddat eller allmänt nät av ett kommunikations- och informationssystem som ackrediterats för att hantera uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller motsvarande eller SECRET UE/EU SECRET eller motsvarande med ska vara förbjuden.

B.10. ***Lagringsmedier för datorer***

39. Lagringsmedier för datorer ska destrueras med hjälp av förfaranden som godkänts av den behöriga säkerhetsmyndigheten.

40. Lagringsmedier för datorer ska återanvändas, placeras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade i enlighet med hanteringsanvisningarna.

B.11. ***Nödlägen***

41. De särskilda förfaranden som beskrivs nedan får tillämpas i en nödsituation, exempelvis under en situation av överhängande eller faktisk kris, en konflikt, eller krig eller under exceptionella operativa omständigheter.

42. Säkerhetsskyddsklassificerade uppgifter får med godkännande av den behöriga myndigheten överföras med användning av kryptoprodukter som har godkänts för en lägre säkerhetsskyddsklassificeringsnivå eller utan kryptering, om en eventuell försening skulle förorsaka större skada än den skada som uppkommer genom ett röjande av det säkerhetsskyddsklassificerade materialet och om

a) sändaren och mottagaren saknar den kryptoutrustning som krävs eller helt och hållet saknar kryptoutrustning, och

b) det säkerhetsskyddsklassificerade materialet inte kan befordras tillräckligt snabbt på annat sätt.

43. Säkerhetsskyddsklassificerade uppgifter som överförs under de omständigheter som anges i punkt 41 får inte vara försedda med någon markering eller några tecken som skiljer dem från ett meddelande som inte är säkerhetsskyddsklassificerat eller som kan skyddas genom någon tillgänglig kryptoprodukt. Mottagarna ska utan dröjsmål underrättas om säkerhetsskyddsklassificeringsnivån på annat sätt.

44. Om punkterna 41 eller 42 tillämpas, ska därefter en rapport lämnas till den behöriga myndigheten.

SÄKERHETSMEDDELANDE 4

FYSISK SÄKERHET

A. **INLEDNING**

I detta säkerhetsmeddelande fastställs säkerhetsprinciperna för att skapa en säker miljö och därmed garantera korrekt behandling av sekretessbelagda uppgifter i Europaparlamentet. Dessa principer, inklusive de som avser teknisk säkerhet, kommer att kompletteras av hanteringsanvisningarna.

B. **HANTERING AV SÄKERHETSRISKER**

1. De risker som de säkerhetsskyddsklassificerade uppgifterna utsätts för ska hanteras som en process. Den processen ska syfta till att identifiera kända säkerhetsrisker och fastställa säkerhetsåtgärder som ska minska riskerna till en acceptabel nivå i enlighet med de grundläggande principer och miniminormer som anges i detta säkerhetsmeddelande samt till att tillämpa åtgärderna i enlighet med begreppet ”säkerhet på djupet” som fastställs i säkerhetsmeddelande 3. Åtgärdernas effektivitet ska utvärderas fortlöpande.

2. Säkerhetsåtgärder för att skydda säkerhetsskyddsklassificerade uppgifter under hela deras livscykel ska stå i proportion till framför allt de berörda uppgifternas eller materialets säkerhetsskyddsklassificeringsnivå, form och volym, läge och konstruktion för de utrymmen där de säkerhetsskyddsklassificerade uppgifterna förvaras och det lokalt bedömda hotet från fientlig och/eller brottslig verksamhet, inklusive spionage, sabotage och terroristverksamhet.

3. Beredskapsplaner ska beakta behovet att skydda säkerhetsskyddsklassificerade uppgifter i krislägen för att förhindra obehörig tillgång eller röjande, eller att okränkbarhet eller tillgänglighet går förlorad.

4. Åtgärder av förebyggande och återställande karaktär för att minimera effekterna av haverier eller tillbud avseende hanteringen och lagringen av säkerhetsskyddsklassificerade uppgifter ska ingå i kontinuitetsplanerna.

C. **ALLMÄNNA PRINCIPER**

5. Uppgifternas klassificerings- eller markeringsnivå ska avgöra vilken skyddsnivå de kommer att omfattas av när det gäller den fysiska säkerheten.

6. Uppgifter som gör säkerhetsskyddsklassificering motiverad ska markeras och hanteras som sådana, oavsett fysisk form. Deras säkerhetsskyddsklassificering ska klart meddelas mottagarna, antingen genom en säkerhetsskyddsmarkering (om uppgifterna levereras i skriftlig form, antingen på papper eller i kommunikations- och informationssystem) eller genom tillkännagivande muntligen (t.ex. i ett samtal eller en föredragning). Säkerhetsskyddsklassificerat material ska bära en fysisk märkning så att dess säkerhetsskyddsklassificering är lätt identifierbar.

7. Sekretessbelagda uppgifter ska inte under några som helst omständigheter läsas på offentliga platser där de kan ses av en enskild individ utan behov av kännedom i tjänsten, t.ex. på tåg, flygplan, kaféer och barer. De får inte förvaras i hotellkassaskåp eller i hotellrum, eller lämnas utan uppsikt på offentliga platser.

D. **SKYLDIGHETER**

8. Enheten för sekretessbelagda uppgifter är ansvarig för att säkerställa den fysiska säkerheten när det gäller hanteringen av de sekretessbelagda uppgifter som förvaras i säkra utrymmen. Enheten för sekretessbelagda uppgifter är också ansvarig för förvaltningen av sina säkra utrymmen.

9. Ansvaret för den fysiska säkerheten när det gäller hanteringen av uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och av ”andra sekretessbelagda uppgifter” åligger respektive instans/befattningshavare inom parlamentet.

10. Direktoratet för säkerhet och riskbedömning ska sörja för den säkerhetsprövning av personal och övriga säkerhetsprövning som behövs för att trygga en säker hantering av sekretessbelagda uppgifter i Europaparlamentet.

11. Direktoratet för informationsteknik ska förorda och säkerställa att alla inrättade eller använda kommunikations- och informationssystem är helt förenliga med säkerhetsmeddelande 3 och respektive hanteringsanvisningar.

E. **SÄKRA UTRYMMEN**

12. Säkra utrymmen får inrättas enligt de tekniska säkerhetsstandarderna och i enlighet med den nivå för sekretessbelagda uppgifter som fastställs i artikel 7.

13. De säkra utrymmena ska certifieras av ackrediteringsmyndigheten för säkerhet och godkännas av säkerhetsmyndigheten.

F. **KONSULTATION AV SEKRETESSBELAGDA UPPGIFTER**

14. När uppgifter som placeras på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” förvaras på enheten för sekretessbelagda uppgifter och måste konsulteras utanför det säkra området, ska enheten för sekretessbelagda uppgifter översända en kopia till respektive behörig tjänsteenhet, som ska se till att konsultationen och hanteringen av dessa uppgifter sker i överensstämmelse med artiklarna 8.2 och 10 i detta beslut och respektive hanteringsanvisningar.

15. När uppgifter som placeras på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” förvaras hos en annan instans/befattningshavare inom parlamentet än enheten för sekretessbelagda uppgifter, ska sekretariatet för den instansen/befattningshavaren inom parlamentet se till att konsultationen och hanteringen av uppgifterna i fråga sker i överensstämmelse med artiklarna 7.3, 8.1, 8.2, 8.4, 9.3, 9.4, 9.5, 10.2–10.6 och 11 i detta beslut och lämpliga hanteringsanvisningar.

16. När uppgifter som placeras på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande och måste konsulteras i det säkra området, ska enheten för sekretessbelagda uppgifter se till att konsultationen och hanteringen av dessa uppgifter sker i överensstämmelse med artiklarna 9 och 10 i detta beslut och lämpliga hanteringsanvisningar.

G. **TEKNISK SÄKERHET**

17. Ackrediteringsmyndigheten för säkerhet är ansvarig för tekniska säkerhetsåtgärder och ska fastställa de lämpliga hanteringsanvisningarna som ska tillämpas.

18. Säkra läsrum för konsultation av uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande eller av ”andra sekretessbelagda uppgifter” ska vara i överensstämmelse med de särskilda tekniska säkerhetsåtgärder som fastställs i hanteringsanvisningarna.

19. Det säkra området ska omfatta följande utrymmen:

a) Ett säkerhetsprövningsrum som ska inrättas i enlighet med de tekniska säkerhetsåtgärder som anges i hanteringsanvisningarna. Tillgången till detta utrymme ska registreras. Säkerhetsprövningsrummet ska uppfylla höga standarder när det gäller identifiering av personer med tillgång, videoregistrering och säkert utrymme där personlig egendom som inte tillåts i de säkrade rummen ska lämnas in (telefoner, pennor, etc.).

b) Ett kommunikationsrum för överföring och mottagande av säkerhetsskyddsklassificerade uppgifter, inklusive krypterade säkerhetsskyddsklassificerade uppgifter, i enlighet med säkerhetsmeddelande 3 och respektive hanteringsanvisningar.

c) Ett säkert arkiv, om ett sådant har godkänts, och certifierade skåp ska användas separat för uppgifter som placerats på säkerhetsskyddsklassificeringsnivåerna RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET EU/EU SECRET eller motsvarande. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRES SECRETUE/EU TOP SECRET eller motsvarande ska placeras i ett separat rum i ett särskilt certifierat skåp. Det enda kompletterande material som ska finnas i detta rum ska vara den supportfacilitet som enheten för sekretessbelagda uppgifter kan använda för att hantera arkivet.

d) Ett registreringsrum som ska tillhandahålla de nödvändiga verktygen för att se till att registreringen kan ske på papper eller elektroniskt och som därför ska förses med de säkrade utrymmen som behövs för att inrätta ett lämpligt kommunikations- och informationssystem. Endast registreringsrummet får innehålla godkänd och ackrediterad utrustning för mångfaldigande (för framställning av kopior på papper eller i elektronisk form). I hanteringsanvisningarna ska specificeras vilken utrustning för mångfaldigande som är godkänd och ackrediterad. Registreringsrummet ska även ha nödvändigt utrymme för lagring och hantering av ackrediterat material för att möjliggöra markering, kopiering och avsändning av säkerhetsskyddsklassificerade uppgifter i fysisk form, allt efter säkerhetsskyddsklassificeringsnivå. Allt ackrediterat material ska definieras av enheten för sekretessbelagda uppgifter och ackrediteras av ackrediteringsmyndigheten för säkerhet, i enlighet med rekommendationerna från den driftsansvariga myndigheten för informationssäkring. Registreringsrummet ska också utrustas med ackrediterade destrueringsanordningar som godkänts på den högsta säkerhetsskyddsklassificeringsnivån enligt beskrivningen i hanteringsanvisningarna. Översättningar av de uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, EU SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska göras i registreringsrummet, inom ramen för ett lämpligt och ackrediterat system. Registreringsrummet ska inrymma arbetsplatser för två översättare ska kunna arbeta med samma dokument samtidigt. En personalmedlem från enheten för sekretessbelagda uppgifter ska vara närvarande.

e) Ett läsrum för vederbörligen behöriga personers individuella konsultation av säkerhetsskyddsklassificerade uppgifter. Läsrummet ska vara tillräckligt stort för två personer, inklusive en personalmedlem från enheten för sekretessbelagda uppgifter som hela tiden ska vara närvarande varje gång säkerhetsskyddsklassificerade uppgifter konsulteras. Säkerhetsskyddsklassificeringsnivån för detta rum ska vara CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller högre. Läsrummet kan utrustas med tempestutrustning, så att elektronisk konsultation vid behov kan möjliggöras i överensstämmelse med uppgifternas säkerhetsskyddsklassificeringsnivå.

f) Ett mötesrum där upp till 25 personer kan diskutera uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET eller motsvarande. Mötesrummet ska innehålla nödvändig teknisk säker och certifierad tolkningsutrustning till och från två språk. När mötesrummet inte används för möten får det även användas som ett extra läsrum för individuell konsultation. I undantagsfall får enheten för sekretessbelagda uppgifter låta mer än en person konsultera säkerhetsskyddsklassificerade uppgifter, förutsatt att alla personer i rummet har samma säkerhetsprövningsnivå och behov av kännedom i tjänsten. Högst fyra personer får ges rätt att konsultera säkerhetsskyddsklassificerade uppgifter samtidigt. Närvaron av tjänstemän från enheten för sekretessbelagda uppgifter ska stärkas.

g) Tekniska säkrade rum med all teknisk utrustning som rör säkerheten i hela det säkra området samt med de säkrade it-servrarna.

20. Det säkra området ska uppfylla internationella säkerhetsnormer och ska certifieras av direktoratet för säkerhet och riskbedömning. Det säkra området ska omfatta följande minimikrav när det gäller den tekniska säkerheten:

a) Larm- och säkerhetsövervakningssystem.

b) Säkerhetsutrustning och nödsystem (tvåvägsvarningssystem).

c) System med övervakningskameror.

d) Intrångsdetekteringssystem.

e) Behörighetskontroll (inklusive ett biometriskt säkerhetssystem).

f) Godsbehållare (containrar).

g) Skåp.

h) Skydd mot elektromagnetism.

21. När ytterligare tekniska säkerhetsåtgärder behövs, kan dessa införas av ackrediteringsmyndigheten i nära samarbete med enheten för sekretessbelagda uppgifter och med godkännande av säkerhetsmyndigheten.

22. Infrastrukturutrustningen får kopplas till de allmänna förvaltningssystemen i den byggnad där det säkra området finns. Den säkerhetsutrustning som avpassats för behörighetskontroll och till kommunikations- och informationssystemet ska dock vara oberoende av alla andra sådana system som finns inom Europaparlamentet.

H. **INSPEKTIONER AV DET SÄKRA OMRÅDET**

23. Inspektioner av det säkra området ska utföras regelbundet av ackrediteringsmyndigheten för säkerhet och på begäran av enheten för sekretessbelagda uppgifter.

24. Ackrediteringsmyndigheten för säkerhet ska utarbeta en checklista för säkerhetsinspektioner beträffande de punkter som ska kontrolleras under en inspektion i enlighet med hanteringsanvisningarna och hålla denna checklista uppdaterad.

I. **TRANSPORTERING AV SEKRETESSBELAGDA UPPGIFTER**

25. När sekretessbelagda uppgifter transporteras ska de vara övertäckta så att de inte går att se. Det ska inte anges att innehållet är sekretessbelagt i enlighet med hanteringsanvisningarna.

26. Endast budbärare eller personal med lämplig säkerhetsbehörighetsnivå får föra med sig uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande.

27. Sekretessbelagda uppgifter får endast sändas via extern post eller personligt överlämnande utanför en byggnad i enlighet med villkoren i hanteringsanvisningarna.

28. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande får aldrig skickas med e-post eller fax, ens via ett ”säkert” e-postsystem eller en kryptofax. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och andra sekretessbelagda uppgifter får skickas med e-post med hjälp av ett ackrediterat krypteringssystem.

J. **LAGRING AV SEKRETESSBELAGDA UPPGIFTER**

29. De sekretessbelagda uppgifternas klassificerings- eller markeringsnivå ska avgöra vilken skyddsnivå de kommer att omfattas av när det gäller lagringen. De ska lagras i den utrustning som certifierats för det ändamålet i enlighet med hanteringsanvisningarna.

30. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande och ”andra sekretessbelagda uppgifter” ska

a) när de inte används lagras i ett låst standardskåp av stål, antingen på ett kontor eller i ett arbetsutrymme,

b) inte lämnas utan uppsikt, såvida de inte korrekt förvaras i ett låst utrymme,

c) inte lämnas på t.ex. ett skrivbord eller bord på ett sådant sätt att de kan läsas eller flyttas av obehöriga personer, t.ex. besökare, lokalvårdare och underhållspersonal,

d) inte visas för obehöriga personer eller diskuteras med dem.

31. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED eller motsvarande, och ”andra sekretessbelagda uppgifter”, ska förvaras endast på sekretariatet för de berörda instanserna/ befattningshavarna inom parlamentet, eller på enheten för sekretessbelagda uppgifter, i enlighet med hanteringsanvisningarna.

32. Uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET eller motsvarande ska

a) lagras i det säkra området, i ett säkerhetsskåp eller valv; i undantagsfall, till exempel om enheten för sekretessbelagda uppgifter är stängd, får de lagras i ett godkänt och certifierat förvaringsskåp på de säkerhetsansvariga tjänsteenheterna,

b) aldrig någonsin lämnas utan uppsikt inom det säkra området utan att först ha låsts in i ett godkänt förvaringsskåp (även vid mycket kort frånvaro),

c) inte lämnas på t.ex. ett skrivbord eller bord på ett sådant sätt att de kan läsas eller flyttas av en obehörig person, även om den ansvariga personalmedlemmen inom enheten för sekretessbelagda uppgifter är kvar i rummet.

Om ett dokument som innehåller säkerhetsskyddsklassificerade uppgifter tas fram elektroniskt inom det säkra området ska datorn låsas, och ingen ska kunna se bildskärmen om upphovsmannen eller den ansvariga personalmedlemmen vid enheten för sekretessbelagda uppgifter lämnar rummet (om så bara en mycket kort stund). Det ska inte anses vara tillräckligt med ett automatiskt säkerhetslås som aktiveras efter några minuter.

SÄKERHETSMEDDELANDE 5

INDUSTRISÄKERHET

A. **INLEDNING**

1. Detta säkerhetsmeddelande gäller enbart säkerhetsskyddsklassificerade uppgifter.

2. I säkerhetsmeddelandet fastställs bestämmelser för genomförande av de gemensamma miniminormer som anges i del 1 i bilaga I till detta beslut.

3. Med industrisäkerhet avses tillämpningen av åtgärder för att garantera att säkerhetsskyddsklassificerade uppgifter skyddas av entreprenörer eller underentreprenörer vid kontraktsförhandlingar och under hela löptiden för kontrakt som kräver säkerhetsskyddsavtal. Sådana kontrakt får inte medföra tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET.

4. Europaparlamentet, som är kontraktsslutande myndighet, ska säkerställa att de miniminormer för industrisäkerhet som fastställs i detta beslut, och som det hänvisas till i kontraktet, följs när industrienheter och andra enheter tilldelas kontrakt som kräver säkerhetsskyddsavtal.

B. **SÄKERHETSINSLAG I ETT KONTRAKT SOM KRÄVER SÄKERHETS-SKYDDSAVTAL**

B.1. ***Handbok om säkerhetsskyddsklassificering***

5. Före ett anbudsförfarande eller tilldelningen av ett kontrakt som kräver säkerhetsskyddsavtal ska Europaparlamentet i egenskap av upphandlande myndighet fastställa säkerhetsskyddsklassificeringen för alla uppgifter som ska lämnas ut till anbudsgivare och entreprenörer, och även säkerhetsskyddsklassificeringen av eventuella uppgifter från entreprenören. Parlamentet ska i detta syfte utarbeta en handbok om säkerhetsskyddsklassificering, vilken ska användas när kontraktet fullgörs.

6. Följande principer ska gälla för fastställande av säkerhetsskyddsklassificeringsnivån för de olika delarna i ett kontrakt som kräver säkerhetsskyddsavtal:

a) När handboken om säkerhetsskyddsklassificering utarbetas ska Europaparlamentet beakta alla relevanta säkerhetsaspekter, inbegripet den säkerhetsskyddsklassificeringsnivå som uppgifternas upphovsman har fastställt och godkänt för användning i kontraktet.

b) Den övergripande säkerhetsskyddsklassificeringsnivån för ett kontrakt får inte vara lägre än den högsta säkerhetsskyddsklassificeringsnivån för någon av dess delar.

B.2. ***Säkerhetsskyddsöverenskommelse***

7. De kontraktsspecifika säkerhetskraven ska anges i en säkerhetsskyddsöverenskommelse. Säkerhetsskyddsöverenskommelsen ska när så är lämpligt omfatta handboken om säkerhetsskyddsklassificering och utgöra en integrerande del av avtalet eller underentreprenörskontraktet.

8. Säkerhetsskyddsöverenskommelsen ska innehålla bestämmelser om att entreprenören och/eller underentreprenören ska uppfylla de miniminormer som fastställs i detta beslut. Underlåtenhet att iaktta dessa miniminormer kan utgöra tillräcklig grund för att häva kontraktet.

B.3. ***Säkerhetsanvisningar för program/projekt***

9. Beroende på omfattningen av program eller projekt som innebär tillgång till eller hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter kan särskilda säkerhetsanvisningar för program/projekt utarbetas av den upphandlande myndighet som utsetts för att förvalta det berörda programmet eller projektet.

C. **SÄKERHETSGODKÄNNANDE AV VERKSAMHETSSTÄLLE**

10. Ett säkerhetsgodkännande av verksamhetsställe ska beviljas av en medlemsstats nationella säkerhetsmyndighet eller annan behörig säkerhetsmyndighet i en medlemsstat som en indikation på, i enlighet med nationella lagar och andra författningar, att en industrienhet eller en annan enhet kan skydda säkerhetsskyddsklassificerade EU-uppgifter med lämplig säkerhetsskyddsklassificeringsnivå CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET eller motsvarande inom sina anläggningar. Bevis för att ett säkerhetsgodkännande av ett verksamhetsställe beviljats ska läggas fram för Europaparlamentet i egenskap av upphandlande myndighet, innan en entreprenör eller underentreprenör, eller potentiella sådana, får eller beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

11. I samband med ett säkerhetsgodkännande av verksamhetsställe är det nödvändigt att

a) utvärdera integriteten hos industrienheten eller varje annan enhet,

b) bedöma ägande, kontroll och/eller möjlighet till otillbörlig påverkan som kan anses utgöra en säkerhetsrisk,

c) kontrollera att industrienheten eller varje annan enhet har infört ett säkerhetssystem vid verksamhetsstället som omfattar alla relevanta säkerhetsåtgärder som är nödvändiga för att skydda uppgifter eller material på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i enlighet med kraven i detta beslut,

d) kontrollera att personalsäkerhetsstatus, med avseende på ledning, ägare och anställda som behöver ha tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, har fastställts i enlighet med kraven i detta beslut,

e) kontrollera att industrienheten eller varje annan enhet har tillsatt en säkerhetsansvarig för verksamhetsstället som inför ledningen svarar för att se till att säkerhetsskyldigheterna uppfylls inom den enheten.

12. I förekommande fall ska Europaparlamentet, i egenskap av upphandlande myndighet, meddela den berörda nationella säkerhetsmyndigheten eller varje annan behörig säkerhetsmyndighet att det krävs ett säkerhetsgodkännande av verksamhetsställe i det förkontraktuella skedet eller för att genomföra kontraktet. Det ska krävas ett säkerhetsgodkännande av verksamhetsställe eller ett personalsäkerhetsgodkännande i det förkontraktuella skedet när säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska tillhandahållas under anbudsförfarandets gång.

13. Den upphandlande myndigheten får inte tilldela den valde anbudsgivaren ett kontrakt som kräver säkerhetsskyddsavtal innan den har fått bekräftelse från den nationella säkerhetsmyndigheten eller någon annan behörig myndighet i den medlemsstat där den berörde entreprenören eller underentreprenören är registrerad att ett giltigt intyg om säkerhetsgodkännande av verksamhetsställe har utfärdats, om ett sådant krävs.

14. Varje behörig säkerhetsmyndighet som har utfärdat ett säkerhetsgodkännande av verksamhetsställe ska meddela Europaparlamentet i egenskap av upphandlande myndighet om alla ändringar som avser detta godkännande. När det gäller underentreprenader ska den behöriga säkerhetsmyndigheten informeras i enlighet med detta.

15. Återkallande av ett säkerhetsgodkännande av verksamhetsställe av en behörig nationell säkerhetsmyndighet eller annan behörig säkerhetsmyndighet ska utgöra tillräcklig grund för att Europaparlamentet, i egenskap av upphandlande myndighet, ska kunna säga upp kontraktet eller utestänga en anbudsgivare från upphandlingsförfarandet.

D. **KONTRAKT OCH UNDERENTREPRENÖRSKONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL**

16. När säkerhetsskyddsklassificerade uppgifter lämnas till en potentiell anbudsgivare i det förkontraktuella skedet ska meddelandet om upphandling innehålla en bestämmelse som förpliktigar en anbudsgivare som inte lämnar något anbud eller väljs ut att inom en bestämd period återlämna alla säkerhetsskyddsklassificerade handlingar.

17. När ett kontrakt eller underentreprenörskontrakt som kräver säkerhetsskyddsavtal har tilldelats ska Europaparlamentet, i egenskap av upphandlande myndighet, underrätta entreprenörens eller underentreprenörens nationella säkerhetsmyndighet och/eller annan behörig säkerhetsmyndighet om säkerhetsbestämmelserna i detta kontrakt.

18. Vid uppsägningen av ett kontrakt ska Europaparlamentet, i egenskap av upphandlande myndighet (och/eller den behöriga säkerhetsmyndigheten, beroende på vad som är lämpligt när det gäller underentreprenader), omedelbart underrätta den nationella säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet i den medlemsstat där entreprenören eller underentreprenören är registrerad.

19. Som en allmän regel ska entreprenören eller underentreprenören vara skyldig att efter slutförandet av den säkerhetsskyddsklassificerade entreprenaden eller underentreprenaden återlämna alla säkerhetsskyddsklassificerade uppgifter till den upphandlande myndigheten.

20. Särskilda bestämmelser för förfogandet över säkerhetsskyddsklassificerade uppgifter under fullgörandet av kontraktet eller sedan det avslutats ska fastställas i säkerhetsskyddsöverenskommelsen.

21. Om entreprenören eller underentreprenören har tillstånd att behålla säkerhetsskyddsklassificerade uppgifter sedan kontraktet har avslutats, ska miniminormerna i detta beslut fortsätta att tillämpas, och konfidentialiteten för de säkerhetsskyddsklassificerade EU-uppgifterna ska skyddas av entreprenören eller underentreprenören.

22. De villkor på vilka entreprenören får anlita underentreprenörer ska fastställas i anbudsinfordran och i kontraktet.

23. En entreprenör ska inhämta tillstånd från Europaparlamentet, i egenskap av upphandlande myndighet, innan delar av kontraktet läggs ut på en underentreprenör. Industrienheter eller andra enheter som är registrerade i en tredjestat får tilldelas underentreprenörskontrakt endast om ett informationssäkerhetsavtal har ingåtts med unionen.

24. Entreprenören ska vara ansvarig för att se till att all underentreprenad utförs i enlighet med miniminormerna i detta beslut och får inte lämna ut säkerhetsskyddsklassificerade EU-uppgifter till en underentreprenör utan föregående skriftligt medgivande från den upphandlande myndigheten.

25. När det gäller säkerhetsskyddsklassificerade uppgifter som framställts eller hanterats av entreprenören eller underentreprenören ska upphovsmannens rättigheter utövas av den upphandlande myndigheten.

E. **BESÖK MED ANKNYTNING TILL KONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL**

26. När Europaparlamentet, entreprenörer eller underentreprenörer kräver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i varandras lokaler för att genomföra ett kontrakt som kräver säkerhetsskyddsavtal, ska besök anordnas i samarbete med de berörda nationella säkerhetsmyndigheterna eller andra behöriga säkerhetsmyndigheter. När det gäller särskilda projekt får dock de nationella säkerhetsmyndigheterna även enas om ett förfarande genom vilket sådana besök kan anordnas direkt.

27. Alla besökare ska inneha ett lämpligt personalsäkerhetsgodkännande och ha behov av kännedom i tjänsten för tillgång till säkerhetsskyddsklassificerade uppgifter med anknytning till Europaparlamentets kontrakt.

28. Besökare ska ges tillgång enbart till säkerhetsskyddsklassificerade uppgifter som har samband med besökets syfte.

F. **ÖVERFÖRING OCH BEFORDRAN AV SÄKERHETSSKYDDS-KLASSIFICERADE UPPGIFTER**

29. Överföringen av säkerhetsskyddsklassificerade uppgifter på elektronisk väg ska omfattas av tillämpliga bestämmelser i säkerhetsmeddelande 3.

30. Transport av säkerhetsskyddsklassificerade uppgifter ska omfattas av tillämpliga bestämmelser i säkerhetsmeddelande 4 och av respektive hanteringsanvisningar.

31. Följande principer ska gälla vid fastställandet av säkerhetsarrangemangen för transport av säkerhetsskyddsklassificerat material som frakt:

a) Säkerheten ska garanteras i alla skeden av transporten, från ursprungsplatsen till slutdestinationen.

b) Den skyddsnivå som ska ges en leverans ska vara den högsta säkerhetsskyddsklassificeringsnivån för det material som leveransen innehåller.

c) Ett säkerhetsgodkännande av verksamhetsställe på lämplig nivå ska inhämtas för företag som sköter transporten. I sådana fall ska den personal som sköter leveransen säkerhetsprövas i enlighet med bilaga I.

d) Innan något material med säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET eller motsvarande förflyttas över en gräns ska avsändaren upprätta en transportplan som ska godkännas av generalsekreteraren.

e) Resorna ska i möjligaste mån ske utan omvägar och slutföras så snabbt som omständigheterna medger.

f) Rutterna ska när det är möjligt förläggas inom medlemsstaternas territorium.

G. **ÖVERFÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER TILL ENTREPRENÖRER I TREDJESTATER**

32. Säkerhetsskyddsklassificerade uppgifter ska överföras till entreprenörer och underentreprenörer i tredjestater i enlighet med säkerhetsbestämmelser som överenskommits mellan Europaparlamentet, i egenskap av upphandlande myndighet, och den berörda tredjestat där entreprenören är registrerad.

H. **HANTERING OCH LAGRING AV UPPGIFTER SOM PLACERATS PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅN RESTREINT UE/EU RESTRICTED**

33. Tillsammans med den nationella säkerhetsmyndigheten ska Europaparlamentet, i egenskap av upphandlande myndighet, när så är lämpligt ha rätt att i enlighet med kontraktsbestämmelserna besöka entreprenörens/underentreprenörens verksamhetsställen för att kontrollera att de nödvändiga säkerhetsåtgärder för skydd av säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED som krävs enligt kontraktet har vidtagits.

34. I den omfattning som krävs enligt nationella lagar och andra författningar ska Europaparlamentet, i egenskap av upphandlande myndighet, underrätta de nationella säkerhetsmyndigheterna eller andra behöriga säkerhetsmyndigheter om kontrakt och underentreprenörskontrakt som innehåller säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

35. Det krävs inte något säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande för entreprenörer eller underentreprenörer och deras personal i fråga om kontrakt som tilldelas av Europaparlamentet och som innehåller säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

36. Europaparlamentet, i egenskap av upphandlande myndighet, ska granska de anbudssvar som inkommit till följd av meddelandena om upphandling och som avser kontrakt som kräver tillgång till säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, utan hinder av de krav på säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande som kan finnas i nationella lagar och andra författningar.

37. De villkor på vilka entreprenören får anlita underentreprenörer ska fastställas i anbudsinfordran och i kontraktet.

38. När ett kontrakt inbegriper hantering av uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED i kommunikations- och informationssystem som sköts av en entreprenör, ska Europaparlamentet i egenskap av upphandlande myndighet se till att kontraktet eller underentreprenörskontraktet specificerar de nödvändiga tekniska och administrativa kraven för ackreditering av kommunikations- och informationssystem i proportion till den uppskattade risken, med beaktande av alla relevanta faktorer. Den upphandlande myndigheten och den berörda nationella säkerhetsmyndigheten ska enas om omfattningen av ackrediteringen av sådana system.

SÄKERHETSMEDDELANDE 6

ÖVERTRÄDELSER AV SÄKERHETSBESTÄMMELSERNA OCH FÖRLUST ELLER RÖJANDE AV SEKRETESSBELAGDA UPPGIFTER

1. En överträdelse av säkerhetsbestämmelserna inträffar som resultat av en handling eller försummelse som begåtts i strid med detta beslut och som kan medföra att sekretessbelagda uppgifter röjs.

2. Röjande av sekretessbelagda uppgifter inträffar när dessa helt eller delvis har kommit i händerna på obehöriga, dvs. personer som vare sig genomgått lämplig säkerhetsprövning eller har behov av kännedom i tjänsten, eller om det är sannolikt att en sådan händelse har inträffat.

3. Sekretessbelagda uppgifter kan röjas till följd av slarv, försummelse eller tanklöshet samt genom åtgärder från organ som riktar sig mot EU, eller genom subversiva organisationer.

4. Om generalsekreteraren upptäcker eller informeras om bevisade eller misstänkta fall av överträdelser av säkerhetsbestämmelserna och förlust eller röjande av sekretessbelagda uppgifter ska han eller hon

a) fastställa fakta,

b) bedöma den skada som skett och försöka minimera den,

c) vidta åtgärder för att förhindra ett upprepande och

d) underrätta den tredje partens behöriga myndighet eller den behöriga myndighet i medlemsstaten som framställt eller översänt de sekretessbelagda uppgifterna.

Om ärendet berör en ledamot av Europaparlamentet, ska generalsekreteraren agera tillsammans med parlamentets talman.

Om uppgifterna tas emot från en annan EU-institution ska generalsekreteraren handla i enlighet med de lämpliga säkerhetsåtgärderna för säkerhetsskyddsklassificerade uppgifter och de arrangemang som fastställts enligt ramavtalet med kommissionen eller det interinstitutionella avtalet med rådet.

5. Alla personer som är skyldiga att hantera sekretessbelagda uppgifter ska grundligt informeras om säkerhetsförfarandena och farorna med oförsiktiga samtal och om sina kontakter med medierna. Vidare ska de där så är lämpligt underteckna en förklaring om att de inte kommer att röja de sekretessbelagda uppgifternas innehåll till tredje personer. I förklaringen ska de även intyga att de kommer att respektera skyldigheterna att skydda säkerhetsskyddsklassificerade uppgifter och att de inser konsekvenserna av att inte göra detta. Om en person som inte har informerats om säkerhetsförfarandena och inte undertecknat motsvarande förklaring tar del av eller använder säkerhetsskyddsklassificerade uppgifter ska detta betraktas som en överträdelse av säkerhetsbestämmelserna.

6. Ledamöter av Europaparlamentet, tjänstemän i parlamentet och övriga parlamentsanställda som arbetar för de politiska grupperna eller uppdragstagare ska omedelbart rapportera till generalsekreteraren om de får vetskap om överträdelser av säkerhetsbestämmelserna och förlust eller röjande av sekretessbelagda uppgifter.

7. Varje person som är ansvarig för att sekretessbelagda uppgifter röjs ska bli föremål för disciplinära åtgärder i enlighet med relevanta bestämmelser. Sådana åtgärder ska inte påverka eventuella rättsliga åtgärder som kan vidtas enligt tillämplig rätt.

8. Utan att det påverkar andra rättsliga åtgärder ska överträdelser som begås av parlamentets tjänstemän eller av parlamentets övriga anställda som arbetar för de politiska grupperna medföra tillämpning av de förfaranden och påföljder som fastställs i avdelning VI i tjänsteföreskrifterna.

9. Utan att det påverkar andra rättsliga åtgärder ska överträdelser som begås av ledamöter av Europaparlamentet behandlas i enlighet med artiklarna 9.2, 152, 153 och 154 i Europaparlamentets arbetsordning.