Europeiska gemenskapernas

officiella tidning

ISSN 1024-3054

L 101

fyrtiofjärde årgången

11 april 2001

Svensk utgåva

Lagstiftning

Innehållsförteckning

Pris: 19,50 EUR

SV

De rättsakter vilkas titlar är tryckta med fin stil är sådana rättsakter som har avseende på den löpande handläggningen av jordbrukspolitiska frågor. De har normalt begränsad giltighetstid.

Beträffande alla övriga rättsakter gäller att titlarna är tryckta med fet stil och föregås av en asterisk.

II

(Rättsakter vilkas publicering inte är obligatorisk)

RÅDET

RÅDETS BESLUT

av den 19 mars 2001

om antagande av rådets säkerhetsbestämmelser

(2001/264/EG)

EUROPEISKA UNIONENS RÅD HAR FATTAT DETTA BESLUT

med beaktande av Fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 207.3 i detta,

med beaktande av rådets beslut 2000/396/EG, EKSG, Euratom av den 5 juni 2000 om antagande av rådets arbetsordning [1], särskilt artikel 24 i denna, och

av följande skäl:

(1) För att kunna utveckla rådets verksamhet på områden som kräver olika grader av sekretess bör ett omfattande säkerhetssystem skapas som omfattar rådet, dess generalsekretariat och medlemsstaterna.

(2) Ett sådant system bör sammanföra alla tidigare beslut och bestämmelser i detta ämne i en enda rättsakt.

(3) I praktiken kommer merparten av EU-uppgifter med beteckningen "CONFIDENTIEL UE" (hemligt) och högre sekretessgrad att röra den gemensamma säkerhets- och försvarspolitiken.

(4) För att garantera det sålunda inrättade säkerhetssystemets effektivitet bör medlemsstaterna knytas till det genom att sådana nationella åtgärder vidtas som krävs för att bestämmelserna i detta beslut skall kunna respekteras, när medlemsstaternas behöriga myndigheter och dess anställda hanterar sekretessbelagda EU-uppgifter.

(5) Rådet välkomnar kommissionens avsikt att senast på tillämpningsdagen för det här beslutet införa ett omfattande system i enlighet med bilagan, för att kunna säkerställa att unionens beslutsprocess fungerar obehindrat.

(6) Rådet betonar vikten av att i förekommande fall låta Europaparlamentet och kommissionen omfattas av de regler och normer för sekretess som är nödvändiga för att skydda unionens och medlemsstaternas intressen.

(7) Detta beslut påverkar inte artikel 255 i fördraget och dess genomförandeinstrument.

(8) Detta beslut påverkar inte gällande praxis i medlemsstaterna när det gäller information till de nationella parlamenten om unionens verksamhet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Rådets säkerhetsbestämmelser som återfinns i bilagan godkänns härmed.

Artikel 2

1. När det gäller hantering av sekretessbelagda EU-uppgifter skall generalsekreteraren/den höge representanten vidta lämpliga åtgärder för att säkerställa att de bestämmelser som avses i artikel 1 respekteras vid rådets generalsekretariat (nedan kallat generalsekretariatet) av generalsekretariatets tjänstemän och övriga anställda, av utomstående uppdragstagare som anlitas av generalsekretariatet och av personal som har avdelats till generalsekretariatet, såväl inom rådets lokaler som i de decentraliserade EU-myndigheterna [2].

[1] EGT L 149, 23.6.2000, s. 21.

[2] Se rådets slutsatser av den 10 november 2000.

2. Medlemsstaterna skall vidta lämpliga åtgärder så att det, i enlighet med nationella ordningar, vid hanterandet av sekretessbelagda EU-uppgifter säkerställs att bestämmelserna i artikel 1 respekteras av medlemsstaternas myndigheter och i deras lokaler av

a) anställda vid medlemsstaternas ständiga representationer vid Europeiska unionen och av de nationella delegationer som deltar i rådsmöten eller i möten i rådsorgan, eller som deltar i annan rådsverksamhet,

b) andra anställda vid medlemsstaternas nationella förvaltningar som hanterar sekretessbelagda EU-uppgifter, oavsett om de tjänstgör på medlemsstaternas territorium eller utomlands,

c) utomstående uppdragstagare som anlitas av medlemsstaterna och avdelad personal från medlemsstaterna som hanterar sekretessbelagda EU-uppgifter.

Medlemsstaterna skall genast informera generalsekretariatet om de åtgärder som vidtagits.

3. De åtgärder som avses under punkterna 1 och 2 skall vara genomförda senast den 30 november 2001.

Artikel 3

I överensstämmelse med de grundläggande principer och miniminormer för säkerhet som återfinns i del I av bilagan, får generalsekreteraren/den höge representanten vidta åtgärder i enlighet med del II, avsnitt 1.1 och 1.2 i bilagan.

Artikel 4

Föreliggande beslut skall från dagen för antagandet ersätta

a) rådets beslut 98/319/EG av den 27 april 1998 om föreskrifter om hur tjänstemän och övriga anställda vid rådets generalsekretariat kan få tillstånd att ha tillgång till sekretessbelagd information som innehas av rådet [1],

b) beslut av generalsekreteraren/höge representanten för den gemensamma utrikes- och säkerhetspolitiken av den 27 juli 2000 om åtgärder för skydd av sekretessbelagda uppgifter, vilka åtgärder skall tillämpas vid rådets generalsekretariat [2],

c) rådets generalsekreterares beslut nr 433/97 av den 22 maj 1997 om förfarandet för säkerhetsprövning av de tjänstemän som ansvarar för Cortesynätets funktion.

Artikel 5

1. Detta beslut skall träda i kraft samma dag det offentliggörs.

2. Det skall tillämpas från den 1 december 2001.

Utfärdat i Bryssel den 19 mars 2001.

På rådets vägnar

A. LINDH

Ordförande

[1] EGT L 140, 12.5.1998, s. 12.

[2] EGT C 239, 23.8.2000, s. 1.

BILAGA

SÄKERHETSBESTÄMMELSER FÖR EUROPEISKA UNIONENS RÅD

INNEHÅLL

Sida

Sida

Tillägg

DEL 1

GRUNDLÄGGANDE PRINCIPER OCH MINIMINORMER FÖR SÄKERHET

INLEDNING

1. I dessa bestämmelser fastställs de grundläggande principer och miniminormer för säkerhet som skall tillämpas av rådet, rådets generalsekretariat (nedan kallat generalsekretariatet), medlemsstaterna och av Europeiska unionens decentraliserade myndigheter (nedan kallade decentraliserade EU-myndigheter) så att säkerheten garanteras och var och en kan vara förvissad om att gemensamma skyddsnormer för säkerheten har fastställts.

2. ”Sekretessbelagda EU-uppgifter” omfattar alla uppgifter och all materiel, som om de röjdes obehörigen skulle kunna skada EU:s intressen i olika hög grad, eller en eller flera av dess medlemsstaters intressen, oavsett om upphovet till uppgifterna finns inom EU eller de har erhållits från en medlemsstat, tredje land eller internationella organisationer.

3. I dessa bestämmelser innebär

   a) *handling:* brev, not, protokoll, rapport, memorandum, signal/meddelande, skiss, foto, diapositiv, film, karta, grafisk framställning, plan, anteckningsblock, stencil, karbonpapper, skrivmaskinsband eller band till skrivare, kassett, diskett eller hårddisk i dator, cd-rom eller annat fysiskt medium på vilket uppgifter har lagrats,

   b) *materiel:* handling enligt definitionen under punkt a samt varje slags utrustning eller vapen som antingen har tillverkats eller håller på att tillverkas.

4. Säkerheten har följande huvudsyften:

   a) att skydda sekretessbelagda EU-uppgifter mot spioneri och mot att de röjs utan tillstånd,

   b) att skydda EU-uppgifter som hanteras i nät och system för kommunikation och information mot hot som riktar sig mot uppgifternas okränkbarhet och tillgänglighet,

   c) att skydda anläggningar där EU-uppgifter förvaras från sabotage och uppsåtlig skada,

   d) om detta misslyckats, bedöma omfattningen och graden av den skada som åsamkats, begränsa följderna av den och vidta åtgärder för att avhjälpa skadan.

5. Grunderna för god säkerhet är följande:

   a) En nationell säkerhetsorganisation i varje medlemsstat som är ansvarig för

      i) insamling och registrering av underrättelser om spioneri, sabotage, terrorism och annan omstörtande verksamhet, och

      ii) information och råd till regeringen och genom denna till rådet, om arten av hotet mot säkerheten och vilka skyddsåtgärder som kan vidtas.

   b) I varje medlemsstat och på generalsekretariatet, en teknisk myndighet för informationssäkerhet (Infosec) som är ansvarig för att tillsammans med den berörda säkerhetsmyndigheten tillhandahålla information och ge råd om tekniska hot mot säkerheten och vilka skyddsåtgärder som kan vidtas.

   c) Regelbundet samarbete mellan ministerier, myndigheter och berörda avdelningar inom generalsekretariatet, för att i tillämpliga fall fastställa och rekommendera

      i) vilka uppgifter, resurser och anläggningar som skall skyddas, och

      ii) gemensamma skyddsnormer.

6. I sekretessfrågor krävs det omsorg och erfarenhet för att kunna välja ut vilka uppgifter och vilken materiel som skall skyddas och bedömningen av vilken skyddsnivå som krävs. Grundläggande är att skyddsnivån skall motsvara känsligheten hos de enskilda uppgifterna och den materiel som skall skyddas. För att säkerställa ett obehindrat uppgiftsflöde skall åtgärder vidtas för att undvika överdriven sekretessbeläggning. Systemet för säkerhetsklassning är det instrument som skall användas för att omsätta principerna i verkligheten; ett liknande system för säkerhetsklassning bör följas i planeringen och organiseringen av hur man förhindrar spioneri, sabotage, terrorism och andra hot, så att de viktigaste utrymmen där sekretessbelagda uppgifter förvaras och de känsligaste punkterna i dessa får högsta möjliga skyddsnivå.

GRUNDLÄGGANDE PRINCIPER

7. **Säkerhetsåtgärderna skall**

a) omfatta alla personer som har tillgång till sekretessbelagda uppgifter, sekretessbelagda informationsbärande medier, alla utrymmen där sådana uppgifter förvaras och viktiga anläggningar,

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

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

d) säkerställa att sekretessbelagda uppgifter sprids endast på grundval av principen ”behöver ha tillgång till uppgifterna för tjänsteutövningen”, som är grundläggande för alla aspekter av säkerhet,

e) Säkerställa okränkbarheten (dvs. förebygga förvanskning, obehörig ändring eller radering) och tillgängligheten (dvs. åtkomst skall inte nekas dem som behöver och är behöriga att få tillgång till alla uppgifter), vare sig uppgifterna är sekretessbelagda eller inte, och särskilt till sådana uppgifter som lagras, bearbetas eller överförs i elektronisk form.

HUR SÄKERHETEN SKALL ORGANISERAS

Gemensamma miniminormer

8. Rådet och varje enskild medlemsstat skall säkerställa att gemensamma miniminormer för säkerhet iakttas i alla förvaltningar och/eller ministerier, andra EU-institutioner, myndigheter och av uppdragstagare så att sekretessbelagda EU-uppgifter kan meddelas i förvissning om att de kommer att hanteras med samma omsorg överallt. Sådana miniminormer skall omfatta kriterier för säkerhetsprövning av personal och förfaranden för skydd av sekretessbelagda EU-uppgifter.

SÄKERHET NÄR DET GÄLLER PERSONALEN

Säkerhetsprövning av personal

9. Alla personer som behöver ha tillgång till uppgifter som fått beteckningen CONFIDENTIEL UE eller en högre sekretessgrad, skall på vederbörligt sätt genomgå en säkerhetsprövning innan tillträde beviljas. En liknande säkerhetsprövning skall krävas för personer i vars tjänsteutövning det ingår tekniskt handhavande av kommunikations- och informationssystem som innehåller sekretessbelagda uppgifter. Syftet med denna säkerhetsprövning skall vara att fastställa om dessa personer

a) är obrottsligt lojala,

b) har en sådan personlighet och en sådan omdömesförmåga att inget tvivel kan uppstå om deras integritet i hanterandet av sekretessbelagda uppgifter, eller

c) kan vara mottagliga för påtryckningar från utländska eller andra källor, till exempel beroende på tidigare bostadsort eller tidigare förbindelser som skulle kunna utgöra en säkerhetsrisk.

Särskilt noggrann granskning inom ramen för säkerhetsprövningen skall göras av personer

d) som skall ha tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET,

e) där tjänsteutövningen medför tillgång till en stor mängd uppgifter som berör EU på nivån SECRET UE,

f) vars tjänsteutövning ger dem särskild tillgång till kommunikations- eller informationssystem som är nödvändiga ur operativ synvinkel och sålunda möjlighet att få obehörig tillgång till stora mängder sekretessbelagda EU-uppgifter, eller att åsamka uppdraget allvarlig skada genom tekniskt sabotage.

Under de omständigheter som det redogörs för under punkterna d–f ovan skall man i största möjliga utsträckning använda sig av tekniken med registerkontroll.

10. När personer som inte behöver ha tillgång till uppgifterna för sin tjänsteutövning skall tas i anspråk under omständigheter då de kan få tillgång till sekretessbelagda EU-uppgifter (t.ex. bud, säkerhetspersonal, underhållspersonal och städare), skall de först genomgå vederbörlig säkerhetsprövning.

Register över säkerhetsprövning av personal

11. Alla avdelningar, organ eller inrättningar som hanterar sekretessbelagda EU-uppgifter eller där det finns kommunikations- eller informationssystem som är nödvändiga ur operativ synvinkel, skall hålla ett register över den personal som varit föremål för säkerhetsprövning. Varje säkerhetsprövning skall kontrolleras när så krävs för att säkerställa att den är relevant för personens aktuella uppdrag. Säkerhetsprövningen skall ses över med förtur när nya uppgifter indikerar att ett fortsatt uppdrag med sekretessbelagda uppgifter inte längre är förenligt med säkerhetsintressena. Registret över de personer som säkerhetsprövats skall hållas av säkerhetschefen för avdelningen, organet eller inrättningen i fråga.

Säkerhetsanvisningar för personalen

12. All personal, vars tjänst innebär att de kan få tillgång till sekretessbelagda uppgifter skall när de börjar sin tjänst få en grundlig genomgång med återkommande repetition av kraven på säkerhet och hur denna säkerhet erhålls. Det är lämpligt att kräva att all sådan personal skriftligen intygar att de är fullt införstådda med de säkerhetsbestämmelser som rör deras tjänst.

Ledningsansvar

13. Arbetsledningen skall ha skyldighet att känna till vilka av personalen som sysslar med klassificerat arbete eller som har tillgång till kommunikations- eller informationssystem som är nödvändiga ur operativ synvinkel och som registrerar och rapporterar om incidenter eller uppenbart sårbara punkter som skulle kunna påverka säkerheten.

Personalens säkerhetsstatus

14. Förfaranden skall fastställas för att säkerställa att det, när negativa uppgifter kommer fram om en person, fastställs huruvida denna person sysslar med sekretessbelagt arbete eller har tillgång till kommunikations- eller informationssystem som är nödvändiga ur operativ synvinkel, och att den berörda myndigheten informeras. Om det fastställs att personen utgör en säkerhetsrisk skall han/hon avstängas eller avlägsnas från sådana uppdrag där han/hon skulle kunna äventyra säkerheten.

FYSISK SÄKERHET

Behov av skydd

15. Den grad av fysiska säkerhetsåtgärder som skall tillämpas för att skydda sekretessbelagda EU-uppgifter skall stå i relation till den säkerhetsklassning, den volym och det hot som föreligger mot befintliga uppgifter och materiel. Säkerhetsklassning på såväl för hög som för låg nivå skall därför motarbetas, och säkerhetsklassningen skall regelbundet ses över. Alla som har tillgång till sekretessbelagda EU-uppgifter skall följa en gemensam praxis när det gäller säkerhetsklassning av dessa uppgifter och följa gemensamma skyddsnormer för hur uppgifter och materiel som kräver skydd skall förvaras, vidarebefordras/överföras och förstöras.

Kontroller

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

Byggnadernas säkerhet

17. Byggnader där sekretessbelagda EU-uppgifter förvaras eller där det finns kommunikations- eller informationssystem som är nödvändiga ur operativ synvinkel, skall skyddas mot obehörigt tillträde. Arten av skydd för sekretessbelagda EU-uppgifter, t.ex. galler för fönster, lås för dörrar, vakter vid ingångarna, automatiska system för kontroll av tillträde, säkerhetskontroller och patruller, larmsystem, system för upptäckt av intrång och vakthundar, skall vara avhängig

a) säkerhetsklassningen på och omfånget av de uppgifter och den materiel som skall skyddas samt var i byggnaden de förvaras,

b) kvaliteten på säkerhetsskåp för uppgifterna och materielen, och

c) byggnadens konstruktion och belägenhet.

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

Beredskapsplaner

19. Detaljerade planer skall utarbetas i förväg för hur sekretessbelagda uppgifter skall skyddas i händelse av en lokal eller nationell kris.

INFORMATIONSSÄKERHET (INFOSEC)

20. Informationssäkerheten rör fastställandet och tillämpningen av säkerhetsåtgärder för att skydda uppgifter som har bearbetats, lagrats eller överförts i kommunikations- och informationssystem eller andra elektroniska system mot sekretessbrott, förlust av okränkbarheten eller tillgängligheten, oavsiktligt eller avsiktligt. Relevanta motåtgärder skall vidtas för att hindra obehöriga från att få tillgång till EU-uppgifter, för att förhindra att behöriga användare nekas tillgång till EU-uppgifter och för att förhindra att EU-uppgifter förvanskas eller obehörigen ändras eller raderas.

ÅTGÄRDER MOT SABOTAGE OCH ANDRA FORMER AV UPPSÅTLIG SKADA

21. Fysiska försiktighetsåtgärder för skydd av viktiga anläggningar där sekretessbelagda uppgifter förvaras är de bästa skyddsåtgärderna mot sabotage och uppsåtlig skada, och de kan inte ersättas med enbart säkerhetsprövning av personal. Det behöriga nationella organet skall samla in underrättelser om spionerі, sabotage, terrorism och annan omstörtande verksamhet.

UTLÄMNANDE AV SEKRETESSBELAGDA UPPGIFTER TILL TREDJE LAND ELLER INTERNATIONELLA ORGANISATIONER

22. Beslutet att lämna ut sekretessbelagda EU-uppgifter där rådet är upphovsman till tredje land eller internationell organisation, skall fattas av rådet. Om rådet inte är upphovsman, skall rådet först söka tillstånd av upphovsmannen. Om det inte går att fastställa vem denne är kommer rådet att påta sig detta ansvar.

23. Om rådet erhåller sekretessbelagda uppgifter från tredje land, internationella organisationer eller annan tredje part, skall dessa uppgifter skyddas i enlighet med den säkerhetsklassning som har gjorts av dem och motsvarande de normer som fastställs i de här bestämmelserna för sekretessbelagda EU-uppgifter, eller motsvarande de strängare normer som tredje part som lämnar ut uppgifterna kan kräva. Ömsesidiga kontroller får genomföras.

24. Ovannämnda principer skall genomföras i enlighet med de detaljerade föreskrifterna i del II.

DEL II

AVSNITT I

HUR SÄKERHETEN SKALL ORGANISERAS I EUROPEISKA UNIONENS RÅD

Generalsekreteraren/den höge representanten

1. Generalsekreteraren/den höge representanten skall

   a) genomföra rådets säkerhetspolitik,

   b) ta ställning till de säkerhetsproblem som rådet eller dess behöriga organ har hänskjutit till honom,

   c) granska frågor som rör förändringar av rådets säkerhetspolitik, i nära samarbete med de nationella säkerhetsmyndigheterna (eller andra lämpliga organ) i medlemsstaterna (nedan kallade nationella säkerhetsmyndigheter). Bilaga I innehåller en förteckning över dessa myndigheter.

2. Generalsekreteraren/den höge representanten skall dessutom vara ansvarig för att

   a) samordna alla säkerhetsärenden som rör rådets verksamhet,

   b) begära att varje medlemsstat upprättar ett centralt register för uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET och kräva att ett sådant register i förekommande fall upprättas i de decentraliserade EU-myndigheterna,

   c) tillställa de utsedda myndigheterna i medlemsstaterna ansökningar om att den nationella säkerhetsmyndigheten gör en säkerhetsprövning av personal som är anställd vid generalsekretariatet, i enlighet med avsnitt VI,

   d) utreda eller begära en utredning om läckor av sekretessbelagda EU-uppgifter, som enligt prima facie-bevis har inträffat vid generalsekretariatet eller vid någon av de decentraliserade EU-myndigheterna,

   e) begära att berörda säkerhetsmyndigheter inleder utredningar när man misstänker läckor av sekretessbelagda EU-uppgifter utanför generalsekretariatet, eller de decentraliserade EU-myndigheterna, och samordna utredningarna när mer än en säkerhetsmyndighet är inblandad,

   f) tillsammans med och i samförstånd med de berörda nationella säkerhetsmyndigheterna periodiskt genomföra granskningar av säkerhetsarrangemangen för skydd av sekretessbelagda EU-uppgifter i medlemsstaterna,

   g) stå i nära kontakt med alla berörda säkerhetsmyndigheter för att få till stånd en övergripande samordning av säkerheten,

   h) ständigt se över rådets säkerhetspolitik och säkerhetsförfaranden och, i förekommande fall, utarbeta lämpliga rekommendationer. I samband med detta skall generalsekreteraren för rådet lägga fram den årliga inspektionsplanen, som utarbetas av rådets generalsekretariats säkerhetsavdelning.

Rådets säkerhetskommitté

3. En säkerhetskommitté skall inrättas. Den skall bestå av företrädare för den behöriga säkerhetsmyndigheten i varje medlemsstat. Ordföranden i kommittén skall vara generalsekreteraren/den höge representanten eller dennes ställföreträdare. Företrädare för decentraliserade EU-myndigheter får också bjudas in att delta när frågor som rör dem diskuteras.

4. Säkerhetskommittén skall sammanträda enligt anvisningar från rådet, på begäran av generalsekreteraren/den höge representanten eller av en nationell säkerhetsmyndighet. Kommittén skall ha befogenhet att granska och bedöma alla säkerhetsfrågor med anknytning till rådets förfaranden och att i förekommande fall lägga fram rekommendationer för rådet. När det gäller generalsekretariatets verksamhet skall kommittén ha befogenhet att utfärda rekommendationer i säkerhetsfrågor till generalsekreteraren/den höge representanten.

Generalsekretariatets säkerhetsavdelning

5. För att uppfylla de skyldigheter som nämns i punkterna 1 och 2 skall generalsekreteraren/den höge representanten kunna utnyttja generalsekretariatets säkerhetsavdelning för samordning, kontroll och genomförande av säkerhetsåtgärder.

6. Chefen för generalsekretariatets säkerhetsavdelning skall vara den främste rådgivaren till generalsekreteraren/den höge representanten i säkerhetsfrågor, och han/hon skall vara sekreterare i säkerhetskommittén. I detta avseende skall han/hon leda uppdateringen av säkerhetsbestämmelserna och samordna säkerhetsåtgärderna med de behöriga myndigheterna i medlemsstaterna, och i förekommande fall med internationella organisationer som är knutna till rådet genom säkerhetsöverenskommelser. Han/hon skall i dessa avseenden agera som sambandsman.

7. Chefen för generalsekretariatets säkerhetsavdelning skall ha ansvaret för godkännande av IT-system och IT-nät vid generalsekretariatet. Chefen för generalsekretariatets säkerhetsavdelning och de berörda nationella säkerhetsmyndigheterna skall, i förekommande fall, tillsammans besluta om godkännande av IT-system och IT-nät som omfattar generalsekretariatet, medlemsstaterna, decentraliserade EU-myndigheter och/eller tredje part (stater eller internationella organisationer).

Decentraliserade EU-myndigheter

8. Varje direktör för en decentraliserad EU-myndighet skall ha ansvaret för genomförandet av säkerheten inom myndigheten. Han/hon utser normalt en medlem av sin personal att vara ansvarig inför honom/henne på detta område. Denne medlem av personalen skall utses till säkerhetstjänsteman.

Medlemsstaterna

9. Varje medlemsstat bör utse en nationell säkerhetsmyndighet som är ansvarig för de säkerhetsarrangemang som rör sekretessbelagda EU-uppgifter ([1]).

10. Inom ramen för varje medlemsstats förvaltning bör medlemsstaternas säkerhetsmyndigheter vara ansvariga för

    a) att upprätthålla säkerheten för sekretessbelagda EU-uppgifter vid nationella ministerier, organ eller myndigheter, offentliga eller privata, inom landet eller utomlands,

    b) att tillåta inrättandet av ett register för uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET (denna befogenhet kan delegeras till den tjänsteman som är ansvarig för kontrollen av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET vid ett centralt register),

    c) den periodiska inspektionen av säkerhetsarrangemangen för sekretessbelagda EU-uppgifter,

    d) att säkerställa att alla medborgare och alla utlänningar som arbetar vid nationella ministerier, organ eller myndigheter som kan få tillgång till EU-uppgifter som säkerhetsklassats som TRÈS SECRET UE/EU TOP SECRET, SECRET UE och CONFIDENTIEL UE, har säkerhetsprövats,

    e) att utarbeta sådana säkerhetsplaner som anses nödvändiga för att förhindra att sekretessbelagda EU-uppgifter hamnar hos obehöriga.

Ömsesidiga säkerhetsinspektioner

11. Periodiska inspektioner av säkerhetsarrangemangen för skydd av sekretessbelagda EU-uppgifter vid generalsekretariatet och medlemsstaternas ständiga representationer vid Europeiska unionen, liksom av medlemsstaternas utrymmen i rådets byggnader, skall utföras av generalsekretariatets säkerhetsavdelning och av de berörda nationella säkerhetsmyndigheterna tillsammans och genom ömsesidig överenskommelse ([2]).

12. Periodiska inspektioner av säkerhetsarrangemangen för skydd av sekretessbelagda EU-uppgifter vid de decentraliserade EU-myndigheterna skall utföras av generalsekretariatets säkerhetsavdelning eller, på generalsekreterarens begäran, av de nationella säkerhetsmyndigheterna i den medlemsstat där myndigheten ligger.

([1]) För en förteckning över nationella säkerhetsmyndigheter som är ansvariga för säkerheten hos sekretessbelagda EU-uppgifter, se tillägg 1.

([2]) Utan att detta inverkar på 1961 års Wienkonvention om diplomatiska förbindelser.

AVSNITT II

SÄKERHETSKLASSNING OCH MARKERINGAR

SEKRETESSGRADER ([1])

Uppgifter kan placeras in i följande sekretessgrader:

1. TRÈS SECRET UE/EU TOP SECRET (kvalificerat hemligt): denna sekretessgrad skall endast användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen synnerligen allvarlig skada (synnerligt men).

2. SECRET UE (hemligt): denna sekretessgrad skall endast användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen allvarlig skada (icke obetydligt men).

3. CONFIDENTIEL UE (hemligt): denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen skada (ringa men).

4. RESTREINT UE (hemligt): denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vara till nackdel för Europeiska unionens eller en eller flera av dess medlemsstaters intressen.

MARKERINGAR

5. En varningsmarkering kan användas för att ange vilket område handlingen omfattar eller särskild spridning, grundad på behovet av att få tillgång till uppgifterna för tjänsteutövningen.

6. Markeringen ESDP/PESD skall göras på handlingar och kopior av dessa som rör unionens eller en eller flera av dess medlemsstaters säkerhet och försvar, eller som rör militär eller icke-militär krishantering.

7. Vissa handlingar med anknytning till system för informationsteknik (IT-system) kan ha en ytterligare markering som medför extra säkerhetsåtgärder enligt vad som fastställs i relevanta bestämmelser.

FASTSTÄLLANDE AV SEKRETESSGRADER OCH MARKERINGAR

8. Sekretessgrad och annan markering skall fastställas och markeras enligt följande:

   a) Handlingar med beteckningen RESTREINT UE, på mekanisk eller elektronisk väg.

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

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

([1]) En jämförande tabell med sekretessgraderna inom EU, Nato, VEU och medlemsstaterna återfinns i bilaga 2.

AVSNITT III

HUR SÄKERHETSKLASSNINGEN SKALL GÅ TILL

1. Uppgifter skall bara sekretessbeläggas när det är nödvändigt. Sekretessgraden skall anges klart och korrekt och skall upprätthållas bara så länge som uppgifterna kräver skydd.

2. Ansvaret för att sekretessbelägga uppgifter och för eventuell senare inplacering i en lägre sekretessgrad eller för hävande av sekretessen ([1]) vilar helt på upphovsmannen.

   Tjänstemän och övriga anställda vid generalsekretariatet skall sekretessbelägga, inplacera i en lägre sekretessgrad eller häva sekretessen på uppdrag av eller efter överenskommelse med sin generaldirektör.

3. De detaljerade förfarandena för hantering av sekretessbelagda handlingar har fått denna inramning för att säkerställa att de får ett lämpligt skydd med hänsyn till de uppgifter de innehåller.

4. Antalet personer som är behöriga att upprätta handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET skall vara så få som möjligt och deras namn skall finnas på en förteckning som upprättats av generalsekretariatet, varje medlemsstat och i förekommande fall av varje decentraliserad EU-myndighet.

TILLÄMPNING AV SÄKERHETSKLASSNING

5. Säkerhetsklassningen av en handling skall fastställas med utgångspunkt från hur känsligt handlingens innehåll är, i enlighet med definitionen i avsnitt II, punkterna 1–4. Det är viktigt att säkerhetsklassningen är korrekt och att den används med urskillning. Detta gäller särskilt säkerhetsgraden TRÈS SECRET UE/EU TOP SECRET.

6. Upphovsmannen till en handling som skall säkerhetsklassas skall ha ovanstående bestämmelser i åtanke och bromsa alla tendenser till för hög eller för låg sekretessgrad.

   Även om en hög säkerhetsnivå vid första anblicken tycks garantera bättre skydd för en handling, kan en rutinmässig klassning med för hög sekretessgrad resultera i att man förlorar förtroendet för giltigheten i säkerhetsklassningssystemet.

   Å andra sidan skall handlingar inte placeras i för låg sekretessgrad bara för att undvika de begränsningar som är förknippade med skydd.

   En praktisk vägledning för säkerhetsklassning finns i bilaga 3.

7. Enstaka sidor, stycken, avsnitt, bilagor, tillägg och bifogade papper till en viss handling kan kräva inplacering i en annan sekretessgrad och skall markeras i enlighet med detta. Säkerhetsklassningen av handlingen som helhet skall vara densamma som den del som fått den högsta sekretessgraden.

8. Säkerhetsklassningen av ett brev eller en not som åtföljer bilagor skall göras i samma sekretessgrad som den högsta sekretessgraden hos bilagorna. Upphovsmannen bör ange tydligt med vilken grad de skall säkerhetsklassas när de skilts från de bifogade handlingarna.

INPLACERING I LÄGRE SEKRETESSGRAD OCH HÄVANDE AV SEKRETESS

9. Sekretessbelagda EU-handlingar kan inplaceras i en lägre sekretessgrad eller bli föremål för sekretessens hävande endast efter tillstånd av den som upprättat handlingarna och, om så krävs, efter diskussion med andra berörda parter. Inplacering i lägre sekretessgrad eller hävande av sekretess skall bekräftas skriftligen. Den institution, den medlemsstat, det organ, den följdorganisation eller högre myndighet som har upprättat handlingen skall ha ansvaret för att informera sina mottagare om förändringen, och dessa skall i sin tur vara ansvariga för att informera eventuella efterföljande mottagare till vilka de har översänt handlingen eller en kopia av den.

10. Upphovsmannen skall, om så är möjligt, på den sekretessbelagda handlingen ange ett datum eller en tidsperiod när uppgifterna får inplaceras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall skall denne se över handlingarna minst vart femte år för att säkerställa att den ursprungliga säkerhetsklassningen fortfarande är nödvändig.

([1]) ”Inplacering i en lägre sekretessgrad” motsvaras av eng. ”downgrading”, fr. ”déclassement”, ”hävande av sekretess” motsvaras av eng. ”declassification”, fr. ”déclassification”.

AVSNITT IV

FYSISK SÄKERHET

ALLMÄNT

1. Det viktigaste syftet med de fysiska säkerhetsåtgärderna är att hindra obehöriga från att få tillgång till sekretessbelagda EU-uppgifter och/eller materiel som är sekretessbelagd.

SÄKERHETSKRAV

2. Alla lokaler, utrymmen, byggnader, kontor, rum, kommunikations- och informationssystem osv. i vilka sekretessbelagda EU-uppgifter och materiel förvaras och/eller hanteras skall skyddas genom lämpliga fysiska säkerhetsåtgärder.

3. När man bestämmer vilken grad av fysiskt säkerhetsskydd som är nödvändigt skall hänsyn tas till relevanta faktorer som

   a) säkerhetsklassningen av uppgifter och/eller materiel,

   b) mängden och formen (t.ex. pappersutskrift, lagring på datormedier) av uppgifterna,

   c) av underrättelsetjänster lokalt bedömt hot som riktar sig mot EU, medlemsstaterna och/eller andra institutioner eller tredje part som innehar sekretessbelagda EU-uppgifter och som innefattar sabotage, terrorism och annan omstörtande och/eller brottslig verksamhet.

4. De fysiska säkerhetsåtgärder som tillämpas skall

   a) förhindra intrång i smyg eller genom tvång,

   b) avskräcka, hindra och avslöja illojala personer (”spionen i huset”),

   c) förhindra att tjänstemän och andra anställda vid generalsekretariatet eller medlemsstaternas ministerier och/eller andra institutioner eller tredje part som inte behöver uppgifterna för tjänstens utövande får tillgång till sekretessbelagda EU-uppgifter.

FYSISKA SÄKERHETSÅTGÄRDER

Säkerhetsutrymmen

5. Utrymmen där uppgifter med beteckningen CONFIDENTIEL UE eller med högre grad av sekretess hanteras och förvaras skall organiseras och struktureras så att de motsvarar något av följande:

   a) Säkerhetsutrymme klass 1: ett utrymme där uppgifter klassade som CONFIDENTIEL UE eller med högre grad av sekretess hanteras och förvaras på ett sådant sätt att tillträde till utrymmet i själva verket innebär tillgång till sekretessbelagda uppgifter. Ett sådant utrymme kräver

      i) en klart fastställd och skyddad yttre gräns genom vilken alla in- och utpasseringar kontrolleras,

      ii) ett kontrollsystem för inpassering, som bara släpper in dem som säkerhetsprövats på vederbörligt sätt och som har särskilt tillstånd att vistas i utrymmet,

      iii) specificering av säkerhetsklassningen av de uppgifter som normalt sett finns i utrymmet, dvs. de uppgifter för vilka tillträde till utrymmet ger tillgång till uppgifterna.

   b) Säkerhetsutrymme klass II: ett utrymme där uppgifter med beteckningen CONFIDENTIEL UE eller högre hanteras och förvaras på ett sådant sätt att det kan skyddas från tillträde av obehöriga genom internt upprättade kontroller, t.ex. lokaler som innehåller enheter där uppgifter med beteckningen CONFIDENTIEL UE eller högre regelbundet hanteras och förvaras. Ett sådant utrymme kräver

      i) en klart fastställd och skyddad yttre gräns genom vilken alla in- och utpasseringar kontrolleras,

      ii) ett kontrollsystem för inpassering som enbart ger tillträde för personer som säkerhetsprövats i vederbörlig ordning och fått särskilt tillstånd att vistas i utrymmet. Alla andra personer skall eskorteras eller kontrolleras på annat sätt för att hindra obehörigt tillträde till sekretessbelagda EU-uppgifter och tillträde till utrymmen som är föremål för tekniska säkerhetsinspektioner.

De utrymmen där tjänstgörande personal inte vistas 24 timmar om dygnet skall inspekteras omedelbart efter den normala arbetstiden för att säkerställa att sekretessbelagda EU-uppgifter är korrekt skyddade.

Administrativt utrymme

6. Kring eller ledande till säkerhetsutrymmen av klass I eller klass II får ett administrativt utrymme med lägre säkerhet upprättas. Detta kräver en synlig gräns som gör att personal och fordon kan kontrolleras. Enbart uppgifter med beteckningen RESTREINT UE skall hanteras och förvaras i administrativa utrymmen.

Kontroll av in- och utpassering

7. Tillträdet till säkerhetsutrymmen av klass I och klass II skall kontrolleras genom passersedel eller genom att den permanenta personalen känner igen personerna. Ett system för kontroll av besökare, för att se till att obehöriga inte får tillträde till sekretessbelagda EU-uppgifter, skall också upprättas. Systemen med passersedel kan kompletteras med automatiserad identifiering, vilken skall ses som ett komplement till, men inte en fullständig ersättning för vakter. En förändring i hotbedömningen kan medföra att åtgärderna för kontroll av in- och utpassering förstärks, till exempel vid besök av prominenta personer.

Patrullering av vakter

8. Patrullering av säkerhetsutrymmen av klass I och klass II skall äga rum utanför normal arbetstid för att skydda EU-tillgångar från att utsättas för fara, skada eller förlust. Hur ofta patrulleringen skall genomföras är avhängigt av de lokala omständigheterna, men som vägledning kan intervallet varannan timme anges.

Säkerhetsskåp och valv

9. Tre klasser av skåp skall användas för förvaring av sekretessbelagda EU-uppgifter:

   — Klass A: säkerhetsskåp som godkänts nationellt för förvaring av uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET i ett säkerhetsutrymme av klass I eller klass II,

   — Klass B: säkerhetsskåp som godkänts nationellt för förvaring av uppgifter med beteckningen SECRET UE och CONFIDENTIEL UE i ett säkerhetsutrymme av klass I eller klass II,

   — Klass C: arkivmöbler som är lämpliga enbart för förvaring av uppgifter med beteckningen RESTREINT UE.

10. För valv som byggts inom ett säkerhetsutrymme av klass I eller klass II och för alla utrymmen av klass I där uppgifter med beteckningen CONFIDENTIEL UE eller högre förvaras på öppna hyllor eller visas på diagram, kartor osv. skall väggarna, golven och taken, dörren eller dörrarna med lås, av en nationell säkerhetsmyndighet ha intygats erbjuda ett skydd som motsvarar den klass säkerhetsskåp som godkänts för förvaring av uppgifter av motsvarande säkerhetsklass.

Lås

11. Lås som används för säkerhetsskåp och valv i vilka sekretessbelagda EU-uppgifter förvaras skall motsvara följande normer:

   — Grupp A: nationellt godkända för skåp av klass A.

   — Grupp B: nationellt godkända för skåp av klass B.

   — Grupp C: enbart avsedda för arkivmöbler av klass C.

Kontroll av lås och kombinationer

12. Lås till säkerhetsskåp får inte avlägsnas från kontorsbyggnaden. Kombinationer till säkerhetsskåp skall memoreras av de personer som behöver känna till dem. För användning i nödsituationer skall den säkerhetsansvarige vid inrättningen i fråga vara ansvarig för reservnycklar och ett skriftligt dokument med varje kombination; dokumenten skall ligga i separata, ogenomskinliga kuvert. Arbetsnycklar, reservsäkerhetsnycklar och kombinationer skall förvaras i separata säkerhetsskåp. Säkerhetsskyddet för dessa lås och kombinationer bör inte vara mindre strängt än de uppgifter som de ger tillgång till.

13. Så få personer som möjligt skall ha kännedom om kombinationer till säkerhetsskåp. Kombinationer skall ställas om

a) vid mottagande av ett nytt skåp,

b) vid byte av personal,

c) vid sekretessbrott eller vid misstanke om detta,

d) helst var sjätte månad eller åtminstone en gång om året.

Anordningar för upptäckt av intrång

14. När larmsystem, interntelevision och andra elektriska anordningar används för att skydda sekretessbelagda EU-uppgifter, skall det finnas ett elektriskt nödsystem för att säkerställa att systemet är operativt även om huvudströmmen bryts. Ett annat grundläggande krav är att tekniskt fel eller manipulation av sådana system skall utlösa larm eller ge en annan pålitlig varning till bevakningspersonalen.

Godkänd utrustning

15. De nationella säkerhetsmyndigheterna skall med egna eller bilaterala medel hålla uppdaterade förteckningar över typer och modeller för den säkerhetsutrustning som de har godkänt för direkt eller indirekt skydd av sekretessbelagda uppgifter under olika specificerade omständigheter och villkor. Generalsekretariatets säkerhetsavdelning skall ha en liknande förteckning, som bland annat grundar sig på information från nationella säkerhetsmyndigheter. De decentraliserade EU-myndigheterna skall rådgöra med generalsekretariatets säkerhetsavdelning och i tillämpliga fall med de nationella säkerhetsmyndigheterna i värdmedlemsstaten innan de köper sådan utrustning.

Fysiskt skydd för kopierings- och faxapparater

16. Kopierings- och faxapparater skall ha det fysiska skydd som krävs för att säkerställa att bara behöriga personer kan använda dem och att alla sekretessbelagda produkter är föremål för riktiga kontroller.

SKYDD MOT ”TJUVTITTANDE” OCH ”TJUVLYSSNANDE”

Tjuvtittande

17. Alla lämpliga åtgärder skall vidtas dag som natt för att garantera att sekretessbelagda EU-uppgifter inte blir tillgängliga, inte ens av misstag, för obehöriga.

Tjuvlyssnande

18. Kontor eller utrymmen där sekretessbelagda EU-uppgifter med beteckningen SECRET UE eller högre regelbundet diskuteras skall skyddas mot ”attacker” av passivt och aktivt tjuvlyssnande när hotbilden kräver det. Den behöriga säkerhetsmyndigheten ansvarar för att bedöma riskerna för sådana attacker, efter samråd med nationella säkerhetsmyndigheter, när så krävs.

19. För att fastställa vilka skyddsåtgärder som skall vidtas i lokaler som är känsliga för passivt tjuvlyssnande (t.ex. isolering av väggar, dörrar, golv och tak, mätningar av det ljud som tränger ut och för aktivt tjuvlyssnande (t.ex. sökning efter mikrofoner) får generalsekretariatets säkerhetsavdelning begära hjälp av de nationella säkerhetsmyndigheterna. Säkerhetsansvariga vid de decentraliserade EU-myndigheterna får begära att tekniska inspektioner utförs av generalsekretariatets säkerhetsavdelning och/eller begära hjälp av experter från de nationella säkerhetsmyndigheterna.

20. När omständigheterna så kräver får telekommunikationsutrustning och elektrisk eller elektronisk kontorsutrustning av alla slag som används under möten på säkerhetsnivån SECRET UE och högre, kontrolleras av tekniska säkerhetsexperter från de nationella säkerhetsmyndigheterna på begäran av den säkerhetsansvarige i fråga.

TEKNISKA SÄKERHETSUTRYMMEN

21. Vissa områden kan betecknas som tekniskt säkra utrymmen. En särskild inpasseringskontroll skall utföras. Sådana utrymmen skall hållas låsta på godkänt sätt när de inte används och alla nycklar skall behandlas som säkerhetsnycklar. Sådana utrymmen skall vara föremål för regelbundna fysiska inspektioner som också skall göras efter varje obehörigt intrång eller misstanke om sådant intrång.

22. En detaljerad inventarieförteckning över utrustning och möbler skall finnas, så att man kan övervaka flyttning av utrustning och möbler. Inga möbler och ingen utrustning skall föras till ett sådant utrymme förrän det har inspekterats omsorgsfullt av särskilt utbildad säkerhetspersonal, för att spåra eventuell avlyssningsutrustning. Som allmän regel gäller att installation av kommunikationslinjer på tekniskt säkra områden bör undvikas.

AVSNITT V

ALLMÄNNA BESTÄMMELSER SOM GÄLLER PRINCIPEN OM ATT BEGRÄNSA TILLGÅNGEN TILL SEKRETESSBELAGD INFORMATION TILL VAD EN TJÄNSTEMAN BEHÖVER VETA FÖR SIN TJÄNSTEUTÖVNING SAMT OM SÄKERHETSPRÖVNING

1. Tillgång till sekretessbelagd EU-information skall beviljas för personer som behöver den för att utföra sina tjänsteåligganden eller uppdrag. Tillgång till uppgifter med sekretessgraderna TRÈS SECRET UE/EU TOP SECRET, SECRET UE och CONFIDENTIEL UE skall endast beviljas för personer som genomgått vederbörlig säkerhetsprövning.

2. Ansvaret att avgöra vad en tjänsteman behöver veta för sin tjänsteutövning skall, allt efter de krav som uppgiften innebär, ligga hos generalsekretariatet, de decentraliserade EU-myndigheterna eller det organ eller den avdelning i en medlemsstat där vederbörande tjänsteman skall vara sysselsatt.

3. Säkerhetsprövning av personal grundad på relevanta gällande förfaranden skall åvila tjänstemannens uppdragsgivare. När det gäller tjänstemän och övriga anställda inom generalsekretariatet anges förfarandet för säkerhetsprövningen i avsnitt VI.

   Säkerhetsprövningen skall leda till att ett ”säkerhetsintyg” utfärdas, i vilket det skall anges vilken nivå av sekretessbelagd information som den person som genomgått säkerhetsprövningen skall få tillgång till samt datum då intyget löper ut.

   Ett säkerhetsintyg för en viss sekretessgrad kan ge innehavaren tillgång till uppgifter med lägre säkerhetsklassning.

4. Personer som inte är tjänstemän eller övriga anställda inom generalsekretariatet eller medlemsstaterna, t.ex. medarbetare, tjänstemän eller anställda inom EU:s institutioner, med vilka man kan behöva diskutera eller för vilka man kan behöva visa sekretessbelagda EU-uppgifter skall ha genomgått säkerhetsprövning för sekretessbelagd EU-information och ha informerats om sitt ansvar för säkerheten. Samma regel skall under liknande förhållanden gälla för utomstående uppdragstagare, experter och konsulter.

SÄRSKILDA BESTÄMMELSER FÖR TILLGÅNG TILL UPPGIFTER MED SEKRETESSGRADEN TRÈS SECRET UE/EU TOP SECRET

5. Samtliga personer som skall få tillgång till information med sekretessgraden TRÈS SECRET UE/EU TOP SECRET skall först ha genomgått säkerhetsprövning för denna grad.

6. Samtliga personer som behöver få tillgång till uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET skall utses av avdelningschefen och deras namn skall införas i det register som är relevant för säkerhetsklassen TRÈS SECRET UE/EU TOP SECRET.

7. Samtliga personer skall innan de får tillgång till uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET underteckna en försäkran om att de informerats om rådets säkerhetsrutiner och att de till fullo är medvetna om sitt särskilda ansvar när det gäller att skydda uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET och de påföljder som i EU:s bestämmelser och i nationell lagstiftning eller nationella förvaltningsbestämmelser föreskrivs om sekretessbelagd information lämnas ut till obehöriga, vare sig detta sker uppsåtligt eller genom försumlighet.

8. Om personer vid möten m.m. ges tillgång till information med sekretessgraden TRÈS SECRET UE/EU TOP SECRET skall den ansvarige säkerhetstjänstemannen inom det organ där dessa personer är verksamma underrätta det organ som anordnat mötet om att de innehar erforderligt tillstånd.

9. Samtliga personer som lämnar en tjänstgöring för vilken de behöver få tillgång till information med sekretessgraden TRÈS SECRET UE/EU TOP SECRET skall avföras från den lista som upprättats för säkerhetsklassen TRÈS SECRET UE/EU TOP SECRET. Dessutom skall alla sådana personer åter göras uppmärksamma på det särskilda ansvar de har när det gäller att skydda uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET. De skall vidare underteckna en försäkran där de förklarar att de varken kommer att använda eller lämna ut någon information med sekretessgraden TRÈS SECRET UE/EU TOP SECRET.

SÄRSKILDA BESTÄMMELSER FÖR TILLGÅNG TILL UPPGIFTER MED SEKRETESSGRAD SECRET UE OCH CONFIDENTIEL UE

10. Samtliga personer som skall få tillgång till information med sekretessgraden SECRET UE eller CONFIDENTIEL UE skall först genomgå säkerhetsprövning för den aktuella säkerhetsnivån.

11. Samtliga personer som får tillgång till information med sekretessgraden SECRET UE eller CONFIDENTIEL UE skall informeras om de aktuella säkerhetsbestämmelserna och skall vara medvetna om konsekvenserna vid försumlighet.

12. Om personer vid möten m.m. ges tillgång till information med sekretessgraden SECRET UE eller CONFIDENTIEL UE skall den ansvarig säkerhetstjänstemannen inom det organ där dessa personer är verksamma underrätta det organ som anordnat mötet om att de innehar erforderligt tillstånd.

SÄRSKILDA BESTÄMMELSER FÖR TILLGÅNG TILL UPPGIFTER MED SEKRETESSGRADEN RESTREINT UE

13. Personer med tillgång till uppgifter med sekretessgraden RESTREINT UE skall göras uppmärksamma på de här säkerhetsbestämmelserna liksom på påföljderna vid försumlighet.

FÖRFLYTTNINGAR

14. Om en medarbetare förflyttas från en tjänst som innebär hantering av sekretessbelagt EU-material skall registret övervaka att materialet på korrekt sätt överlämnas från den avgående till den tillträdande tjänstemannen.

SÄRSKILDA ANVISNINGAR

15. Personer som det åligger att hantera sekretessbelagd EU-information skall när de inleder sin tjänstgöring och därefter med regelbundna intervall göras uppmärksamma på

    a) de hot mot säkerheten som oförsiktiga samtal innebär,

    b) de försiktighetsmått som de bör vidta i sitt umgänge med pressen,

    c) det hot som kommer från underrättelseorgan som inriktar sig på EU och medlemsstaterna för att få kännedom om sekretessbelagd information och verksamhet inom EU,

    d) skyldigheten att genast rapportera till vederbörande säkerhetsmyndigheter alla närmanden eller förhållningssätt som kan föranleda misstanke om spioneri eller eventuella onormala förhållanden som kan ha relevans för säkerheten.

16. Alla personer som normalt upprätthåller täta kontakter med företrädare för länder vilkas underrättelseorgan inriktar sig på EU och medlemsstaterna för att få kännedom om sekretessbelagd information och verksamhet inom EU, skall informeras om den teknik man vet att olika underrättelseorgan använder sig av.

17. Det finns inga säkerhetsbestämmelser inom rådet för privata resor till något som helst resmål för de personer som genomgått säkerhetsprövning för tillgång till sekretessbelagd EU-information. De behöriga säkerhetsmyndigheterna skall dock informera de tjänstemän och övriga anställda som de har ansvar för om sådana regler för resor som de kan komma att omfattas av. Säkerhetstjänstemännen ansvarar för att hålla fortbildningsmöten med personalen om dessa särskilda anvisningar.

AVSNITT VI

FÖRFARANDE FÖR SÄKERHETSPRÖVNING AV GENERALSEKRETARIATETS TJÄNSTEMÄN OCH ÖVRIGA ANSTÄLLDA

1. Endast generalsekretariatets tjänstemän och övriga anställda eller personer som arbetar inom generalsekretariatet, som på grund av sina åligganden och för sin tjänsteutövning behöver känna till eller använda sekretessbelagda uppgifter som innehas av rådet, skall ha tillgång till sådana uppgifter.

2. För att få tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET, SECRET UE och CONFIDENTIEL UE måste de personer som avses i punkt 1 ha fått tillstånd i enlighet med det förfarande som avses i punkterna 4 och 5.

3. Tillstånd skall endast ges till personer som har genomgått säkerhetsprövning av de behöriga nationella myndigheterna i medlemsstaterna, i enlighet med förfarandet i punkterna 6-10.

4. Tillsättningsmyndigheten skall, enligt artikel 2 första stycket i tjänsteföreskrifterna, ha ansvar för utfärdandet av de tillstånd som avses i punkterna 1–3.

   Tillsättningsmyndigheten skall bevilja tillstånd efter att ha erhållit yttrande från medlemsstaternas behöriga nationella myndigheter på grundval av den säkerhetsprövning som genomförts i enlighet med punkterna 6–12.

5. Tillståndet, som skall vara giltigt för en period av fem år, får inte ha längre varaktighet än de uppgifter på vars grundval det beviljades. Det får förnyas av tillsättningsmyndigheten i enlighet med förfarandet i punkt 4.

   Tillståndet skall dras in av tillsättningsmyndigheten när den anser att det finns rättmätiga skäl att göra detta. Alla beslut om indragning av ett tillstånd skall meddelas den berörda personen, som kan anhålla om att höras av tillsättningsmyndigheten, och den behöriga nationella myndigheten.

6. Säkerhetsprövningen syftar till att säkerställa att det inte finns några invändningar mot att den berörda personen får tillgång till sekretessbelagda uppgifter som innehas av rådet.

7. Säkerhetsprövningen skall, med den berörda personens medverkan och på begäran av tillsättningsmyndigheten, utföras av behöriga nationella myndigheter i den medlemsstat där den person som skall ges tillstånd är medborgare. Om den berörda personen är bosatt på en annan medlemsstats territorium, kan de berörda nationella myndigheterna uppta samarbete med myndigheterna i den stat där den berörda personen har sin hemvist.

8. Som en del av prövningsförfarandet skall den berörda personen anmodas att fylla i ett formulär med personliga uppgifter.

9. Tillsättningsmyndigheten skall i sin begäran specificera typen av och nivån på de sekretessbelagda uppgifter som den berörda personen skall ha tillgång till så att de behöriga nationella myndigheterna kan genomföra processen med säkerhetsprövning och ge sitt utlåtande om på vilken nivå det är lämpligt att bevilja den personen tillstånd.

10. Hela processen med säkerhetsprövning, tillsammans med de erhållna resultaten, skall genomföras i enlighet med de relevanta regler och bestämmelser som gäller i den berörda medlemsstaten, inklusive de som gäller överklaganden.

11. När medlemsstatens behöriga nationella myndigheter avger ett positivt yttrande får tillsättningsmyndigheten ge den berörda personen tillstånd.

12. Ett negativt yttrande från de behöriga nationella myndigheterna skall meddelas den berörda personen som kan begära att få höras av tillsättningsmyndigheten. Om tillsättningsmyndigheten anser det nödvändigt får den anhålla hos de behöriga nationella myndigheterna om eventuella ytterligare förtydliganden från dessa. Om den negativa uppfattningen bekräftas skall tillstånd inte beviljas.

13. Alla personer som beviljats tillstånd enligt punkterna 4 och 5 skall, när tillståndet beviljas och därefter med jämna mellanrum, erhålla alla nödvändiga föreskrifter angående skyddet av sekretessbelagda uppgifter och hur ett sådant skydd kan garanteras. Dessa personer skall underteckna en förklaring om att de erkänner att de mottagit föreskrifterna och att de åtar sig att lyda dem.

14. Tillsättningsmyndigheten skall vidta alla nödvändiga åtgärder för att genomföra detta avsnitt, bland annat när det gäller reglerna för tillgång till förteckningen över personer med tillstånd.

15. Tillsättningsmyndigheten kan undantagsvis och om tjänsten så kräver, efter att i förväg ha informerat de behöriga myndigheterna om detta och om dessa inte har hört av sig inom en månad, utfärda ett tillfälligt tillstånd för en tidsperiod som inte får överstiga tre månader i avvaktan på resultatet av den undersökning som anges i punkt 7.

16. De preliminära och tillfälliga tillstånd som utfärdas på detta sätt skall inte ge tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET; tillgång till dessa uppgifter skall begränsas till tjänstemän som verkligen har genomgått säkerhetsprövning med positivt resultat, i enlighet med punkt 7. I avvaktan på resultatet av säkerhetsprövningen får de tjänstemän, för vilka det krävs tillstånd för tillgång till uppgifter på nivån TRÈS SECRET UE/EU TOP SECRET, tillfälligt och preliminärt ges tillstånd att få tillgång till uppgifter upp till och med nivån SECRET UE.

AVSNITT VII

UPPRÄTTANDE, UTLÄMNANDE, VIDAREBEFORDRAN/ÖVERFÖRING, FÖRVARING OCH FÖRSTÖRING AV SEKRETESSBELAGDA EU-HANDLINGAR

Innehåll

Allmänna bestämmelser

I detta avsnitt preciseras åtgärderna för upprättande, utlämnande, vidarebefordran/överföring, förvaring och förstöring av sekretessbelagda EU-handlingar enligt punkt 3 a i de grundläggande principerna och miniminormerna för säkerhet som återfinns i del I i denna bilaga. De skall användas som referens för antagande av dessa åtgärder för annan sekretessbelagd EU-materiel alltefter typen av materiel och från fall till fall.

Kapitel I

Upprättande och utlämnande av sekretessbelagda EU-handlingar

UPPRÄTTANDE

1. EU:s säkerhetsklassningar och markeringar skall tillämpas enligt avsnitt II och anges centrerat i marginalen upptill och nedtill på varje sida och varje sida skall numreras. På varje sekretessbelagd EU-handling skall ett referensnummer och ett datum anges. När det gäller handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET och SECRET UE skall detta referensnummer anges på varje sida. Om flera kopior skall lämnas ut skall ett kopienummer anges på första sidan på varje exemplar tillsammans med uppgift om det totala antalet sidor. Alla bilagor och bifogade handlingar skall anges på den första sidan av en handling med beteckningen CONFIDENTIEL UE eller högre sekretessgrad.

2. Handlingar med beteckningen CONFIDENTIEL UE eller högre sekretessgrad får skrivas ut, översättas, förvaras, kopieras, mångfaldigas magnetiskt eller mikrofilmas endast av personer som har genomgått säkerhetsprövning för tillgång till sekretessbelagda EU-uppgifter upp till minst den lämpliga sekretessgraden för handlingen i fråga, utom i det speciella fall som beskrivs i punkt 27 i detta avsnitt.

   De bestämmelser som reglerar datoriserad framställning av sekretessbelagda handlingar fastställs i avsnitt XI.

UTLÄMNANDE

3. Sekretessbelagda EU-uppgifter skall lämnas ut endast till personer som behöver känna till uppgifterna för sin tjänsteutövning och som har genomgått lämplig säkerhetsprövning. Det första utlämnandet skall specificeras av upphovsmannen.

4. Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET skall lämnas ut genom registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET (se avsnitt VIII). När det gäller meddelanden med beteckningen TRÈS SECRET UE/EU TOP SECRET får det behöriga registret ge chefen för kommunikationscentrumet behörighet att framställa det antal kopior som specificeras i mottagarförteckningen.

5. Handlingar med beteckningen SECRET UE eller med lägre sekretessgrad får lämnas vidare av den ursprunglige mottagaren till andra mottagare på grundval av behovet att få uppgifterna för tjänsteutövningen. Upphovsmyndigheterna skall dock tydligt ange eventuella förbehåll som de önskar införa. När sådana förbehåll införs får mottagarna lämna handlingarna vidare endast med upphovsmyndigheternas tillstånd.

6. Alla handlingar med beteckningen CONFIDENTIEL UE eller med högre sekretessgrad skall när de anländer till eller lämnar en inrättning diarieföras av inrättningens register. Anvisningar om vilka uppgifter som skall införas (referenser, datum och vid behov kopienummer) skall vara sådana att handlingarna kan identifieras och de skall införas i ett diarium eller på särskilda skyddade databaserade medier.

Kapitel II

Vidarebefordran/överföring av sekretessbelagda EU-handlingar

EMBALLERING

7. Handlingar med beteckningen CONFIDENTIEL UE eller med högre sekretessgrad skall vidarebefordras i motståndskraftiga, ogenomskinliga dubbla kuvert. Det inre kuvertet skall märkas med lämplig EU-säkerhetsklassning och om möjligt med fullständiga anvisningar om mottagarens tjänstetitel och adress.

8. Det inre kuvertet får endast öppnas av en kontrolltjänsteman vid registret eller dennes ersättare som skall bekräfta mottagandet av de bifogade handlingarna, om inte detta kuvert är adresserat till en person. I sådant fall skall det lämpliga registret diarieföra kuvertets ankomst, och endast den person som det är adresserat till får öppna det inre kuvertet och erkänna mottagandet av de handlingar som det innehåller.

9. Ett mottagningsbevis skall placeras i det inre kuvertet. Mottagningsbeviset, som inte skall vara sekretessbelagt, skall innehålla uppgifter om handlingens referensnummer, datum och kopienummer, men aldrig ärendet.

10. Det inre kuvertet skall placeras i ett ytterkuvert som skall ha ett emballeringsnummer så att mottagningsbeviset kan fyllas i. Säkerhetsklassningen får under inga omständigheter anges på ytterkuvertet.

11. För handlingar med beteckningen CONFIDENTIEL UE eller med högre sekretessgrad skall kurirer och bud erhålla mottagningsbevis med angivande av emballeringsnumren.

VIDAREBEFORDRAN INOM EN BYGGNAD ELLER ETT BYGGNADSKOMPLEX

12. Inom en viss byggnad eller ett visst byggnadskomplex får sekretessbelagda handlingar befordras i ett förseglat kuvert med endast adressatens namn, på villkor att det befordras av en person som genomgått lämplig säkerhetsprövning.

VIDAREBEFORDRAN AV EU-HANDLINGAR INOM ETT LAND

13. Inom ett land får handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET endast befordras med ett officiellt budföretag, eller med personer som är behöriga att få tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET.

14. När budföretag används för vidarebefordran av en handling med beteckningen TRÈS SECRET UE/EU TOP SECRET utanför gränserna för en byggnad eller ett byggnadskomplex, skall bestämmelserna angående emballage och mottagande uppfyllas enligt det här kapitlet. Budföretag skall ha en sådan personal att det garanteras att emballage som innehåller handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET ständigt står under direkt övervakning av en ansvarig tjänsteman.

15. Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET får undantagsvis befordras av tjänstemän, inte bud, utanför en byggnad eller ett byggnadskomplex för lokal användning vid möten och diskussioner förutsatt att

    a) tjänstemannen som agerar bud är behörig att få tillgång till dessa handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET,

    b) befordringssättet uppfyller nationella bestämmelser för vidarebefordran av nationella handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET,

    c) tjänstemannen under inga omständigheter lämnar handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET utan uppsikt,

    d) det vidtas arrangemang för en förteckning över de handlingar som befordras på detta sätt och som skall finnas tillgänglig i registret för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET och som skall diarieföras och kontrolleras mot detta register när handlingarna återkommer.

16. Inom ett visst land får handlingar med beteckningarna SECRET UE och CONFIDENTIEL UE befordras antingen med post, om detta är tillåtet enligt nationella bestämmelser och överensstämmer med villkoren i dessa bestämmelser, eller med bud eller med personer som genomgått säkerhetsprövning för behörighet att få tillgång till sekretessbelagda EU-uppgifter.

17. Varje medlemsstat eller decentraliserad EU-myndighet bör utarbeta föreskrifter för den personal som befordrar sekretessbelagda EU-handlingar på grundval av dessa bestämmelser. Det skall vara ett krav att budet läser och undertecknar dessa föreskrifter. Av föreskrifterna skall det särskilt framgå att handlingarna under inga omständigheter får

    a) lämnas utan uppsikt av budet om de inte är i säkert förvar i enlighet med bestämmelserna i avsnitt IV,

    b) lämnas utan uppsikt i allmänna transportmedel eller privata fordon eller på sådana platser som hotell eller restauranger. De får inte förvaras i kassaskåp på hotell eller lämnas utan uppsikt i hotellrum,

    c) läsas på allmänna platser, t.ex. i flygplan eller på tåg.

VIDAREBEFORDRAN FRÅN EN MEDLEMSSTAT TILL EN ANNAN

18. Materiel med beteckningen CONFIDENTIEL UE eller högre sekretessgrad bör befordras från en medlemsstat till en annan med diplomat- eller militärkurir.

19. Den personal som befordrar materiel med beteckningen SECRET UE och CONFIDENTIEL UE har tillåtelse att göra detta om villkoren är sådana att det garanteras att de inte kan falla i händerna på någon obehörig.

20. Nationella säkerhetsmyndigheter får ge tillåtelse till befordran via personal när diplomat- eller militärkurirer inte är tillgängliga, eller när användningen av sådana kurirer skulle resultera i en försening som skulle vara skadlig för EU:s insatser och när den avsedda mottagaren brådskande behöver materielen. Varje medlemsstat bör utarbeta föreskrifter som omfattar befordran via personal på internationell nivå av sekretessbelagd materiel upp till och med beteckningen SECRET UE av personer som inte är diplomat- eller militärkurirer. Enligt föreskrifterna skall det krävas att

a) budet har genomgått lämplig säkerhetsprövning som har genomförts av medlemsstaterna,

b) ett lämpligt organ eller register förtecknar allt materiel som befordras på detta sätt,

c) paket eller säckar som innehåller EU-materiel är försedda med ett officiellt sigill för att förhindra eller avhålla från tullinspektion samt är märkta med identifikation och föreskrifter till upphittaren,

d) budet bär med sig ett kuririntyg och/eller tjänsteuppdrag som är erkänt av alla EU-staterna och som ger honom behörighet att befordra paketet enligt identifikation,

e) ingen icke EU-medlemssstat eller gräns korsas vid resa på land om inte den stat som befordrar handlingen har en särskild garanti från den staten,

f) budets researrangemang, med tanke på vilka destinationer, resvägar och befordringsvägar som används, står i överensstämmelse med EU:s bestämmelser eller – om nationella bestämmelser för sådana frågor är strängare – i enlighet med sådana bestämmelser,

g) materiel får inte lämnas utan uppsikt av budet om den inte förvaras i enlighet med bestämmelserna för säker förvaring i avsnitt IV,

h) materiel får inte lämnas utan uppsikt i allmänna eller privata fordon, eller på platser som t.ex. restauranger och hotell. Den får inte förvaras i hotellkassaskåp eller lämnas utan uppsikt i hotellrum,

i) om den befordrade materielen innehåller handlingar får dessa inte läsas på offentliga platser (t.ex. i flygplan, på tåg osv.).

Den person som utsetts att befordra den sekretessbelagda materielen måste läsa och underteckna säkerhetsinstruktioner som innehåller minst de föreskrifter som förtecknas ovan samt förfaranden som skall följas i en nödsituation eller om paketet som innehåller den sekretessbelagda materielen efterfrågas av tullen eller säkerhetstjänstemännen vid en flygplats.

VIDAREBEFORDRAN AV HANDLINGAR MED BETECKNINGEN RESTREINT UE

21. Inga särskilda bestämmelser har fastställts för befordran av handlingar med beteckningen RESTREINT UE, utom att de bör vara sådana att det garanteras att de inte kan falla händerna på någon obehörig.

SÄKERHET NÄR DET GÄLLER KURIRER

22. Alla kurirer och sändebud som anlitas för att befordra handlingar med beteckningarna SECRET UE och CONFIDENTIEL UE skall ha genomgått lämplig säkerhetsprövning.

Kapitel III

Teknisk överföring på elektronisk eller annan väg

23. Säkerhetsåtgärderna för kommunikationer är avsedda att garantera en säker överföring av sekretessbelagda EU-uppgifter. De detaljerade regler som skall tillämpas vid överföring av sådana sekretessbelagda EU-uppgifter behandlas i avsnitt XI.

24. Endast godkända kommunikationscentrum och nät och/eller terminaler och system får överföra uppgifter med beteckningarna CONFIDENTIEL UE och SECRET UE.

Kapitel IV

Extra exemplar och översättningar av utdrag från sekretessbelagda EU-handlingar

25. Endast upphovsmannen får ge tillåtelse till kopiering eller översättning av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET.

26. Om personer som inte genomgått säkerhetsprövning för sekretessgraden TRÈS SECRET UE/EU TOP SECRET behöver information som, trots att den finns i en handling med beteckningen TRÈS SECRET UE/EU TOP SECRET, inte har den säkerhetsklassningen, får chefen för registret för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET ges behörighet att framställa det erforderliga antalet utdrag från denna handling. Samtidigt skall han/hon vidta nödvändiga åtgärder för att garantera att dessa utdrag ges lämplig säkerhetsklassning.

27. Handlingar med beteckningen SECRET UE eller lägre sekretessgrad får mångfaldigas och översättas av adressaten, inom ramen för de nationella säkerhetsbestämmelserna och på villkor att det är helt förenligt med principen om behovet av att få kännedom om uppgifterna för tjänsteutövningen. De säkerhetsåtgärder som skall tillämpas på ursprungshandlingen skall även tillämpas på kopior och/eller översättningar. Decentraliserade EU-myndigheter skall följa de här säkerhetsbestämmelserna.

Kapitel V

Granskning och kontroll, förvaring och förstöring av sekretessbelagda EU-handlingar

GRANSKNING OCH KONTROLL

28. Varje år skall alla register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET enligt avsnitt VIII genomföra en systematisk granskning av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET i enlighet med bestämmelserna i avsnitt VIII, punkterna 9-11. Sekretessbelagda EU-handlingar med lägre sekretessgrad än TRÈS SECRET UE/EU TOP SECRET skall underkastats interna kontroller i enlighet med nationella riktlinjer och, när det gäller generalsekreterarens eller EU:s decentraliserade myndigheter, i enlighet med föreskrifter från generalsekreteraren/den höge representanten.

Dessa åtgärder skall ge möjlighet att säkerställa innehavarnas åsikter avseende

a) möjligheten att inplacera i en lägre sekretessgrad eller häva sekretessen för vissa handlingar,

b) handlingar som skall förstöras.

ARKIVERING AV SEKRETESSBELAGDA EU-UPPGIFTER

29. För att minimera förvaringsproblemen skall kontrolltjänstemännen vid alla register ha behörighet att mikrofilma handlingar med beteckningarna TRÈS SECRET UE/EU TOP SECRET, SECRET UE och CONFIDENTIEL UE eller att annars arkivera med hjälp av magnetiska eller optiska medier, förutsatt att

a) mikrofilmnings- eller arkiveringsprocessen företas av personal som har genomgått aktuell säkerhetsprövning för motsvarande säkerhetsklassningsnivå,

b) mikrofilm- eller arkiveringsmediet inplaceras i samma sekretessgrad som originalhandlingarna,

c) mikrofilmning eller arkivering av alla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET rapporteras till upphovsmannen,

d) filmrullar eller annan typ av stöd endast innehåller handlingar med samma säkerhetsklassning, dvs. TRÈS SECRET UE/EU TOP SECRET, SECRET UE eller CONFIDENTIEL UE,

e) mikrofilmning eller arkivering av en handling med beteckningen TRÈS SECRET UE/EU TOP SECRET eller SECRET UE anges tydligt i det register som används för den årliga inventeringen,

f) originalhandlingar som har mikrofilmats eller på annat sätt arkiverats, förstörs i enlighet med bestämmelserna i punkterna 31–36 nedan.

30. Dessa bestämmelser skall även tillämpas på alla andra former av arkivering som är tillåtna av de nationella säkerhetsmyndigheterna, t.ex. med hjälp av elektromagnetiska medier och optisk skiva.

RUTINMÄSSIG FÖRSTÖRING AV SEKRETESSBELAGDA EU-HANDLINGAR

31. För att förebygga onödig anhopning av sekretessbelagda EU-handlingar skall de handlingar som betraktas som föråldrade och till antalet överflödiga av chefen för den inrättning som innehar dem, förstöras så snart som möjligt på följande sätt:

a) Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET får endast förstöras av det centrala registret med ansvar för dessa. Varje förstörd handling skall förtecknas i ett intyg över förstöring som undertecknas av kontrolltjänstemannen för beteckningen TRÈS SECRET UE/EU TOP SECRET och av den tjänsteman som bevittnar förstöringen. Dessa personer skall ha genomgått säkerhetsprövning för sekretessgraden TRÈS SECRET UE/EU TOP SECRET. Det skall göras en notering i registret om detta.

b) Registret skall bevara intygen om förstöring, tillsammans med distributionslistorna under tio år. Kopior skall översändas till upphovsmannen eller till det lämpliga centrala registret endast på uttrycklig begäran.

c) Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, inklusive allt sekretessbelagt material från upprättandet av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, t.ex. dåliga kopior, arbetsutkast, maskinskrivna noter och karbonpapper, skall förstöras under överinseende av en tjänsteman för sekretessgraden TRÈS SECRET UE/EU TOP SECRET genom att brännas, omvandlas till pappersmassa, gå genom en dokumentförstörare eller på annat sätt reduceras så att de är oigenkännliga och icke möjliga att återställa.

32. Handlingar med beteckningen SECRET UE skall förstöras av det register som är ansvarigt för dessa handlingar, under överinseende av en person som har genomgått säkerhetsprövning, enligt någon av de procedurer som anges i punkt 31 c. Handlingar med beteckningen SECRET UE som förstörs skall förtecknas på undertecknade intyg om förstöring vilka skall bevaras av registret tillsammans med distributionslistorna under minst tre år.

33. Handlingar med beteckningen CONFIDENTIEL UE skall förstöras av det register som har ansvar för dessa handlingar, under överinseende av en person som har genomgått säkerhetsprövning, med hjälp av någon av de processer som anges i punkt 31 c. Förstöringen skall registreras i enlighet med nationella bestämmelser och, när det gäller generalsekretariatets eller EU:s decentraliserade myndigheter, i enlighet med instruktioner från generalsekreteraren/den höge representanten.

34. Handlingar med beteckningen RESTREINT UE skall förstöras av det register som har ansvar för dessa handlingar eller av användaren, i enlighet med nationella bestämmelser och, när det gäller generalsekretariatets eller EU:s decentraliserade myndigheter, i enlighet med föreskrifter från generalsekreteraren/den höge representanten.

FÖRSTÖRING I EN NÖDSITUATION

35. Generalsekretariatets, medlemsstaternas och EU:s decentraliserade myndigheter skall utarbeta planer på grundval av lokala förhållanden för att skydda sekretessbelagd EU-materiel i en kris, inklusive förstöring vid behov i en nödsituation samt planer för bortförande; de skall inom sina respektive organisationer utarbeta de föreskrifter som bedöms nödvändiga för att hindra sekretessbelagda EU-uppgifter från att falla i händerna på obehöriga.

36. Arrangemangen för att skydda och/eller förstöra materiel med beteckningarna SECRET UE och CONFIDENTIEL UE i en kris skall under inga omständigheter kunna inverka ogynnsamt på skyddet eller förstöringen av materiel med beteckningen TRÈS SECRET UE/EU TOP SECRET, inklusive krypteringsutrustning, vars behandling skall prioriteras framför alla andra uppgifter. De åtgärder som skall vidtas för att skydda och förstöra krypteringsutrustning i en nödsituation skall omfattas av ad hoc-föreskrifter.

Kapitel VI

Särskilda regler som skall tillämpas på handlingar avsedda för rådet

37. Enheten för sekretessbelagda uppgifter skall inom generalsekretariatet säkerställa att uppgifter i rådets handlingar med beteckningen SECRET UE eller CONFIDENTIEL UE, övervakas.

Under överinseende av generaldirektören för personal och administration skall denna enhet

a) sköta diarieföringen, mångfaldigandet, översättningen, vidarebefordran/överföringen, expedieringen och förstöringen av uppgifterna,

b) se till att förteckningen över sekretessbelagda uppgifter uppdateras,

c) regelbundet fråga dem som upprättat handlingarna huruvida det är nödvändigt att bibehålla säkerhetsklassningen av uppgifterna, och

d) i samråd med säkerhetsavdelningen fastställa praktiska tillvägagångssätt för sekretessbeläggning och hävande av sekretessen.

38. Enheten för sekretessbelagda uppgifter skall föra ett diarium som innehåller följande information:

a) det datum då handlingen med sekretessbelagda uppgifter upprättats,

b) sekretessgraden,

c) den tidpunkt då sekretessen skall hävas,

d) namn på den som upprättat handlingen och vid vilken avdelning detta gjorts,

e) mottagaren eller mottagarna, med angivande av ordningsnummer,

f) ämne,

g) nummer,

h) antal distribuerade exemplar,

i) upprättande av förteckningarna över de sekretessbelagda uppgifter som lagts fram för rådet,

j) register över hävande av sekretessen för och inplacering i en lägre sekretessgrad av sekretessbelagda uppgifter.

39. De allmänna reglerna i kapitel I-V i detta avsnitt skall tillämpas på enheten för sekretessbelagda uppgifter vid generalsekretariatet, om de inte ändras av de särskilda bestämmelser som fastställs i detta kapitel.

AVSNITT VIII

REGISTER FÖR HANDLINGAR MED BETECKNINGEN TRÈS SECRET UE/EU TOP SECRET

1. Syftet med att ha ett register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET är att garantera diarieföring, registrering, hantering och vidarebefordran/överföring av dessa handlingar i enlighet med säkerhetsbestämmelserna. Chefen för registret för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, i varje medlemsstat respektive i generalsekretariatet och vid behov i EU:s decentraliserade myndigheter, kommer att vara kontrolltjänstemannen för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET.

2. De centrala registren kommer att vara huvudsakliga mottagare och expedierande myndighet i medlemsstaterna, i generalsekretariatet och i EU:s decentraliserade myndigheter, där sådana register har upprättats samt vid behov i andra EU-institutioner, internationella organisationer och tredje länder med vilka rådet har överenskommelser om säkerhetsförfaranden för utbyte av sekretessbelagda uppgifter.

3. Vid behov skall det inrättas underavdelningar till registren som skall ha ansvar för den interna förvaltningen av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET; de skall föra uppdaterade register över utlämnandet av de handlingar som förvaras på underavdelningens ansvar.

4. Underavdelningar till registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET skall inrättas enligt avsnitt I för att tillgodose långsiktiga behov och skall vara kopplade till ett centralt register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET. Om handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET behöver konsulteras temporärt får dessa handlingar lämnas ut utan att det inrättas någon underavdelning till ett register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET under förutsättning att det fastställs regler för att garantera att de fortfarande kontrolleras av ett lämpligt register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET och att alla fysiska och personalmässiga säkerhetsåtgärder iakttas.

5. Underavdelningar till registren får inte vidarebefordra/överföra handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET direkt till andra underavdelningar till samma centrala register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET utan uttrycklig tillåtelse från det senare.

6. All utväxling av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET mellan underavdelningar som inte är kopplade till samma centrala register skall gå via de centrala registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET.

CENTRALA REGISTER FÖR HANDLINGAR MED BETECKNINGEN TRÈS SECRET UE/EU TOP SECRET

7. I egenskap av kontrolltjänsteman skall chefen för det centrala registret för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET ha ansvar för

   a) att vidarebefordra/överföra handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET i enlighet med de bestämmelser som fastställs i avsnitt VII,

   b) att upprätta en förteckning över alla underavdelningar till register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET tillsammans med de utnämnda kontrolltjänstemännens och deras behöriga ombuds namn och namnteckningar,

   c) att förvara mottagningsbevis från registren för alla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET som cirkulerats av det centrala registret,

   d) att upprätta ett register över förvarade och cirkulerade handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET,

   e) att upprätta en uppdaterad förteckning över alla de centrala registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET med vilka han/hon vanligtvis korresponderar, tillsammans med de utnämnda kontrolltjänstemännens och deras behöriga ombuds namn och namnteckningar,

   f) att fysiskt skydda alla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET i registret i enlighet med bestämmelserna i avsnitt IV.

UNDERAVDELNINGAR TILL REGISTREN FÖR HANDLINGAR MED BETECKNINGEN TRÈS SECRET UE/EU TOP SECRET

8. I egenskap av kontrolltjänsteman skall chefen för underavdelningen till registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET ha ansvar för

   a) att vidarebefordra handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET i enlighet med bestämmelserna i avsnitt VII och punkterna 5 och 6 i avsnitt VIII,

b) hålla en uppdaterad förteckning över alla personer under honom/henne som är behöriga att få tillgång till uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET,

c) att lämna ut handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET i enlighet med upphovsmannens föreskrifter eller på grundval av behovet av att få information för tjänsteutövningen sedan han/hon först kontrollerat att mottagaren har genomgått erforderlig säkerhetsprövning,

d) att hålla ett uppdaterat register över alla handlingar som han/hon ansvarar för med beteckningen TRÈS SECRET UE/EU TOP SECRET som förvaras eller lämnas ut eller som har översänts till andra register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET och att förvara alla motsvarande mottagningsbevis,

e) att hålla en uppdaterad förteckning över register över handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET med vilka han/hon är behörig att utväxla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, tillsammans med deras kontrolltjänstemäns och behöriga ombuds namn och underskrifter,

f) att fysiskt skydda alla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET som förvaras av registret i enlighet med bestämmelserna i avsnitt IV.

INVENTERINGAR

9. Var tolfte månad skall alla register över handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET genomföra en specificerad inventering av alla handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET som de har ansvar för. En handling anses falla under ett registers ansvar om registret fysiskt förvarar handlingen eller har ett mottagningsbevis från det register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET till vilket handlingen har vidarebefordrats/överförts, ett intyg om att handlingen förstörts eller en föreskrift att inplacera denna handling i en lägre sekretessgrad eller att häva sekretessen.

10. Underavdelningar till register skall sända resultatet av sin årliga inventering till det centrala register som de är ansvariga inför vid en tidpunkt som skall fastställas av det senare.

11. De nationella säkerhetsmyndigheterna samt de EU-institutioner, internationella organisationer och decentraliserade EU-myndigheter där ett centralt register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET har inrättats, skall sända resultatet av de årliga inventeringar som genomförs i de centrala registren för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET till generalsekreteraren/den höge representanten senast den 1 april varje år.

AVSNITT IX

SÄKERHETSÅTGÄRDER SOM SKALL TILLÄMPAS VID SÄRSKILDA MÖTEN SOM ÄGER RUM UTANFÖR RÅDETS LOKALER VILKA INBEGRIPER MYCKET KÄNSLIGA FRÅGOR

ALLMÄNT

1. När Europeiska rådet, rådsmöten, ministermöten eller andra viktiga möten äger rum utanför rådets lokaler i Bryssel och Luxemburg och när det berättigas av de särskilda säkerhetskrav som gäller mycket känsliga frågor eller uppgifter, skall de säkerhetsåtgärder som beskrivs nedan vidtas. Dessa åtgärder gäller endast skyddet av sekretessbelagda EU-uppgifter och andra säkerhetsåtgärder måste eventuellt planeras.

ANSVAR

Värdmedlemsstater

2. Den medlemsstat på vars territorium mötet äger rum (värdmedlemsstat) skall i samarbete med generalsekretariatets säkerhetsavdelning ha ansvar för säkerheten vid Europeiska rådet, rådsmöten, ministermöten eller andra viktiga möten, liksom för den fysiska säkerheten för huvuddelegaterna och deras personal.

När det gäller skyddet av säkerheten skall det i synnerhet garanteras att

a) planer utarbetas för att hantera hot mot säkerheten och incidenter som har samband med säkerhet, och dessa åtgärder skall i synnerhet omfatta en säker förvaring av sekretessbelagda EU-handlingar på avdelningarna,

b) åtgärder vidtas för att möjliggöra tillträde till rådets kommunikationssystem för mottagande och vidarebefordran av sekretessbelagda EU-meddelanden. Värdmedlemsstaten kommer även att vid behov tillhandahålla säkra telefonsystem.

Medlemsstaterna

3. Medlemsstaternas myndigheter bör vidta nödvändiga åtgärder för att garantera att

a) de nationella delegaterna har lämpligt intyg över säkerhetsprövning, vid behov elektroniskt eller via fax, antingen direkt till säkerhetstjänstemannen vid mötet eller via generalsekretariatets säkerhetsavdelning,

b) alla specifika hot meddelas värdmedlemsstatens myndigheter och vid behov generalsekretariatets säkerhetsavdelning, så att lämpliga åtgärder kan vidtas.

Säkerhetstjänsteman vid möten

4. En säkerhetstjänsteman bör utnämnas med ansvar för det övergripande utarbetandet och kontrollen av generella interna säkerhetsåtgärder och för samordningen med andra berörda säkerhetsmyndigheter. De åtgärder som han/hon vidtar skall i allmänhet gälla följande:

a) i) Skyddsåtgärder på mötesplatsen för att garantera att mötet genomförs utan incidenter som kan äventyra säkerheten för sekretessbelagda EU-uppgifter som eventuellt används där.

ii) Kontroll av den personal som har tillträde till mötesplatsen, delegationernas utrymmen och konferensrummen samt kontroll av all utrustning.

iii) Ständig samordning med värdmedlemsstatens behöriga myndigheter och med generalsekretariatets säkerhetsavdelning.

b) Införlivande av säkerhetsföreskrifter i mötets dossier med vederbörlig hänsyn tagen till kraven i de här säkerhetsbestämmelserna och till alla andra säkerhetsföreskrifter som anses nödvändiga.

Generalsekretariatets säkerhetsavdelning

5. Generalsekretariatets säkerhetsavdelning skall vara rådgivare om säkerhet vid mötets förberedande; avdelningen bör företrädas där för att vid behov bistå och ge råd till mötets säkerhetstjänsteman och delegationerna.

6. Varje delegation bör till varje möte utse en säkerhetstjänsteman som kommer att vara ansvarig för behandlingen av säkerhetsfrågor inom sin delegation och för upprätthållande av förbindelsen med säkerhetstjänstemannen vid mötet samt, vid behov, med företrädaren för generalsekretariatets säkerhetsavdelning.

SÄKERHETSÅTGÄRDER

Säkerhetsutrymmen

7. Följande säkerhetsutrymmen bör inrättas:

   a) Ett säkerhetsutrymme i klass II som består av ett planeringsrum, generalsekretariatets kontor och reproduktionsutrustning samt delegationernas kontor vid behov.

   b) Ett säkerhetsutrymme i klass I som består av konferensrummet och tolkarnas och ljudingenjörernas kabiner.

   c) Administrativa utrymmen som består av pressens utrymme och de delar av mötesplatsen som används för administration, servering och inkvartering samt utrymmet i omedelbar anslutning till presscentrumet och mötesplatsen.

Passersedel

8. Mötets säkerhetstjänsteman bör dela ut lämpliga besöksbrickor på begäran av delegationerna i enlighet med deras behov. Det får vid behov göras åtskillnad när det gäller tillträde till olika säkerhetsutrymmen.

9. Enligt säkerhetsföreskrifterna för mötet bör det krävas att alla berörda personer ständigt och på ett tydligt sätt bär och uppvisar sina besöksbrickor inom mötesplatsen så att de vid behov kan kontrolleras av säkerhetspersonalen.

10. Förutom deltagare med besöksbrickor bör så få personer som möjligt ha tillträde till mötesplatsen. Nationella delegater som önskar ta emot besökande under mötet bör underrätta mötets säkerhetstjänsteman. Besökande bör erhålla en besöksbricka. En passersedel för besökande med hans/hennes namn och namnet på den person som besöks bör ifyllas. Besökande skall alltid åtföljas av en säkerhetsvakt eller av den person som tar emot besök. Den besökandes passersedel bör bäras av den ledsagande personen som skall återlämna den, tillsammans med den besökandes besöksbricka, till säkerhetspersonalen när den besökande lämnar mötesplatsen.

Kontroll av foto- och AV-utrustning

11. Kameror eller inspelningsutrustning får inte medföras till ett säkerhetsutrymme i klass I, med undantag av utrustning som medförts av fotografer och ljudingenjörer med vederbörligt tillstånd från mötets säkerhetstjänsteman.

Kontroll av portföljer, bärbara datorer och paket

12. Innehavare av passersedel med tillträde till ett säkerhetsutrymme får vanligtvis medföra sina portföljer och bärbara datorer (endast med egen strömförsörjning) utan att de kontrolleras. När det gäller paket till delegationer får delegationerna ta emot leverans av paket som antingen inspekteras av delegationens säkerhetstjänsteman, undersöks med specialutrustning eller öppnas av säkerhetspersonalen för inspektion. Om mötets säkerhetstjänsteman anser det nödvändigt får det fastställas strängare åtgärder för inspektion av portföljer och paket.

Teknisk säkerhet

13. Mötesrummet får göras tekniskt säkert av en teknisk säkerhetsgrupp som även får genomföra elektronisk övervakning under mötet.

Delegationernas handlingar

14. Delegationerna bör ansvara för att ta sekretessbelagda EU-handlingar till och från möten. De skall även ha ansvar för dessa handlingars kontroll och säkerhet under deras användning i de lokaler som de fått sig tilldelade. Man får anhålla om värdmedlemsstaternas hjälp för befordran av sekretessbelagda handlingar till och från mötesplatsen.

Säker förvaring av handlingar

15. Om generalsekretariatet, kommissionen eller delegationerna inte kan förvara sina sekretessbelagda handlingar i enlighet med godkända normer får de, mot mottagningsbevis, samla dessa handlingar i ett förseglat kuvert hos mötets säkerhetstjänsteman, så att denne kan förvara handlingarna i enlighet med godkända normer.

Inspektion av kontor

16. Mötets säkerhetstjänsteman bör se till att generalsekretariatets och delegationernas kontor inspekteras vid slutet av varje arbetsdag för att garantera att alla sekretessbelagda EU-handlingar förvaras på säker plats; om inte bör han vidta erforderliga åtgärder.

Bortskaffande av sekretessbelagt EU-material

17. Allt material skall behandlas som sekretessbelagt och papperskorgar eller säckar bör överlämnas till generalsekretariatet och delegationerna för bortskaffande. Generalsekretariatet och delegationerna bör, innan de lämnar de lokaler som de fått sig tilldelade, ta sitt skräp till mötets säkerhetstjänsteman som skall se till att det förstörs enligt bestämmelserna.

18. Vid mötets slut bör alla handlingar som generalsekretariatet eller delegationerna förfogar över men inte längre önskar behandlas som makulatur. Det bör göras en noggrann genomsökning av generalsekretariatets och delegationernas lokaler innan de säkerhetsåtgärder som antagits för mötet hävs. Handlingar för vilka ett mottagningsbevis undertecknades bör såvitt det är möjligt förstöras enligt föreskrifterna i avsnitt VII.

AVSNITT X

SEKRETESSBROTT OCH RÖJANDE AV SEKRETESSBELAGDA EU-UPPGIFTER

1. Sekretessbrott inträffar som resultatet av en handling eller försummelse som står i strid med rådets eller nationella säkerhetsbestämmelser vilket kan medföra att sekretessbelagda EU-uppgifter röjs.

2. Röjande av sekretessbelagda EU-uppgifter inträffar när dessa helt eller delvis har fallit i händerna på obehöriga, dvs. personer som inte genomgått vare sig lämplig säkerhetsprövning eller behöver uppgifterna för sin tjänsteutövning eller om det är sannolikt att en sådan händelse har inträffat.

3. Sekretessbelagda EU-uppgifter kan röjas till följd av slarv, försummelse eller tanklöshet samt genom åtgärder från avdelningar vilka riktar sig mot EU eller dess medlemsstater, när det gäller sekretessbelagda EU-uppgifter, eller genom subversiva organisationer.

4. Det är av vikt att alla personer av vilka det krävs att de skall hantera sekretessbelagda EU-uppgifter noggrant informeras om säkerhetsförfaranden, om farorna med obetänksamma samtal och om deras förbindelser med pressen. De bör vara medvetna om vikten av att de genast rapporterar alla sekretessbrott som de eventuellt får vetskap om till säkerhetsmyndigheten i den medlemsstat, den institution eller det organ där de är anställda.

5. När en säkerhetsmyndighet upptäcker eller informeras om ett sekretessbrott som gäller sekretessbelagda EU-uppgifter eller förlust eller försvinnande av sekretessbelagt EU-materiel skall den vidta lämpliga åtgärder för att

   a) fastställa fakta,

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

   c) förebygga en upprepning,

   d) informera lämpliga myndigheter om effekten av sekretessbrott.

   I detta sammanhang skall följande uppgifter tillhandahållas:

   i) En beskrivning av de relevanta uppgifterna, inklusive säkerhetsklassning, referens och kopienummer, datum, upphovsman, ämne och räckvidd.

   ii) En kort beskrivning av omständigheterna vid sekretessbrott, inklusive datum för och den period under vilken uppgifterna eventuellt röjdes.

   iii) Ett uttalande om huruvida upphovsmannen har underrättats.

6. Det skall åligga varje säkerhetsmyndighet att, så snart som den underrättats om att ett sådant sekretessbrott kan ha inträffat, omedelbart rapportera detta och därvid använda följande förfarande: underavdelningen av registret för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET skall rapportera saken till generalsekretariatets säkerhetsavdelning via sitt centrala register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET; vid röjande av sekretessbelagda EU-uppgifter som inträffar inom en medlemsstats behörighetsområde skall det rapporteras till generalsekretariatets säkerhetsavdelning, enligt punkt 5, genom den ansvariga nationella säkerhetsmyndigheten.

7. De fall som gäller uppgifter med beteckningen RESTREINT UE behöver rapporteras endast när de uppvisar ovanliga kännetecken.

8. När generalsekreteraren/den höge representanten underrättas om att ett sekretessbrott har ägt rum skall denne

   a) underrätta den myndighet som var upphovsman till de sekretessbelagda uppgifterna i fråga,

   b) anmoda lämpliga säkerhetsmyndigheter att inleda utredningar,

   c) samordna undersökningarna när mer än en säkerhetsmyndighet berörs,

d) erhålla en rapport om omständigheterna kring brottet, datum för och den period under vilken det kan ha ägt rum och om upptäckten, med en detaljerad beskrivning av innehållet i och säkerhetsklassningen av det berörda materielet. Den skada som åsamkats EU:s intressen eller en eller flera av medlemsstaterna och de åtgärder som vidtagits för att förhindra en upprepning bör även rapporteras.

9. Upphovsmyndigheten skall underrätta adressaterna och ge lämpliga föreskrifter.

10. Varje person som är ansvarig för röjande av sekretessbelagda EU-uppgifter skall underkastas disciplinära åtgärder enligt de relevanta reglerna och bestämmelserna. Sådana åtgärder skall inte påverka eventuella rättsliga åtgärder.

AVSNITT XI

SKYDD FÖR UPPGIFTER SOM HANTERAS I IT- OCH KOMMUNIKATIONSSYSTEM

Innehåll

Kapitel I

Inledning

ALLMÄNT

1. Säkerhetsstrategin och säkerhetskraven i detta avsnitt skall tillämpas på alla kommunikations- och informationssystem och kommunikations- och informationsnät (nedan kallade system) i vilka EU-uppgifter med sekretessgraden CONFIDENTIEL UE och högre hanteras.

2. För system i vilka EU-uppgifter med sekretessgraden RESTREINT UE hanteras krävs också säkerhetsåtgärder för att bevara dessa uppgifters sekretess. För alla system krävs säkerhetsåtgärder för att skydda okränkbarheten och tillgängligheten av dessa system och de uppgifter de innehåller. De säkerhetsåtgärder som skall tillämpas på dessa system skall fastställas av den ackrediteringsmyndighet för säkerhet som har utsetts samt motsvara den bedömda risken och överensstämma med den strategi som anges i de här säkerhetsbestämmelserna.

3. För sensorsystem som innehåller inbyggda IT-system skall skyddet fastställas och specificeras inom den allmänna ramen för de system de tillhör och i så stor utsträckning som möjligt med hjälp av tillämpliga bestämmelser i detta avsnitt.

HOT MOT SYSTEM OCH SYSTEMENS SÅRBARHET

4. Ett hot kan allmänt definieras som en möjlighet till oavsiktligt eller avsiktligt äventyrande av säkerheten. När det gäller system innebär ett sådant äventyrande att en eller flera av egenskaperna sekretess, okränkbarhet och tillgänglighet går förlorade. Sårbarhet kan definieras som en svaghet i kontrollerna eller en avsaknad av kontroller som kan underlätta eller möjliggöra att ett hot sätts i verket mot en specifik tillgång eller ett specifikt mål. Sårbarhet kan vara en försummelse eller höra samman med brister i en kontrolls verkningsfullhet, fullständighet eller konsekvens; den kan vara av teknisk, förfarandemässig eller operativ art.

5. Sekretessbelagda och icke-sekretessbelagda EU-uppgifter som hanteras i system i koncentrerad form för snabb sökning, kommunikation och användning är sårbara i många avseenden. Det finns bland annat en risk för att obehöriga användare får tillgång till uppgifter eller omvänt att behöriga användare vägras tillgång. Det föreligger också risk för obehörigt röjande eller obehörig förvanskning, ändring eller radering av uppgifterna. Den komplicerade och ibland ömtåliga utrustningen är dessutom dyr och ofta svår att snabbt reparera eller ersätta. Dessa system är därför attraktiva mål för verksamhet som går ut på att samla in underrättelser eller sabotage, särskilt om säkerhetsåtgärderna tros vara ineffektiva.

SÄKERHETSÅTGÄRDER

6. Huvudsyftet med de säkerhetsåtgärder som anges i detta avsnitt är att de skall ge skydd mot obehörigt röjande av uppgifter (sekretessbrott) och mot förlust av uppgifternas okränkbarhet och tillgänglighet. För att system som hanterar sekretessbelagda EU-uppgifter skall få tillräckligt säkerhetsskydd skall lämpliga normer för konventionell säkerhet specificeras tillsammans med lämpliga särskilda säkerhetsförfaranden och säkerhetstekniker som är särskilt utformade för varje system.

7. En väl avvägd uppsättning säkerhetsåtgärder skall fastställas och genomföras så att det skapas en säker driftsmiljö för systemet. Dessa åtgärder skall tillämpas på fysiska faktorer, personal, icke-tekniska förfaranden samt driftsmetoder för datorer och kommunikation.

8. Det kommer att krävas åtgärder för datasäkerhet (säkerhetsegenskaper för maskinvara och programvara) för att genomföra principen om behov av uppgifterna för tjänsteutövningen och för att förhindra eller upptäcka obehörigt röjande av uppgifter. När säkerhetskraven fastställs skall det avgöras hur tillförlitliga åtgärderna för datasäkerhet är. Ackrediteringsförfarandet skall avgöra att säkerhetsnivån är tillräckligt hög för att man skall kunna lita på åtgärderna för datasäkerhet.

REDOVISNING AV SYSTEMSPECIFIKA SÄKERHETSKRAV

9. För alla system som hanterar EU-uppgifter med sekretessgraderna CONFIDENTIEL UE och högre skall det krävas att en redovisning av systemspecifika säkerhetskrav utarbetas av myndigheten för driften av IT-system, vid behov med indata och bistånd från projektpersonalen och myndigheten för informationssäkerhet, liksom att den godkänns av ackrediteringsmyndigheten för säkerhet. En redovisning av systemspecifika säkerhetskrav skall också krävas när ackrediteringsmyndigheten för säkerhet bedömer att tillgängligheten och okränkbarheten av EU-uppgifter med sekretessgraden RESTREINT UE eller icke sekretessbelagda EU-uppgifter kan äventyras.

10. Redovisningen av systemspecifika säkerhetskrav skall utarbetas så snart som ett projekt inleds och utvecklas och förbättras allteftersom projektet fortskrider, så att den kan fullgöra olika uppgifter i olika skeden av projektet och av systemets livscykel.

11. Redovisningen av systemspecifika säkerhetskrav skall utgöra den bindande överenskommelse mellan myndigheten för driften av IT-system och ackrediteringsmyndigheten för säkerhet mot vilken systemet skall ackrediteras.

12. Redovisningen av systemspecifika säkerhetskrav skall vara en fullständig och tydlig redovisning av vilka säkerhetsprinciper som skall följas och vilka detaljerade säkerhetskrav som skall uppfyllas. Den skall bygga på rådets säkerhetsstrategi och riskbedömning, eller på parametrar som omfattar driftsmiljön, den lägsta nivån på säkerhetsprövningen av personal, den högsta sekretessgraden för de uppgifter som hanteras, den säkra driftsformen eller kraven på användare. Redovisningen av systemspecifika säkerhetskrav är en integrerad del av den projektdokumentation som skall lämnas till de relevanta myndigheterna för tekniska ändamål, budgetändamål och för godkännande av säkerheten. I sin slutliga utformning utgör redovisningen av systemspecifika säkerhetskrav en fullständig redovisning av vad det innebär att systemet är säkert.

SÄKRA DRIFTSFORMER

13. Alla system som hanterar EU-uppgifter med sekretessgraden CONFIDENTIEL UE och högre skall ackrediteras för drift i en eller, om detta är motiverat på grund av krav under olika tidsperioder, flera av följande säkra driftsformer eller deras nationella motsvarigheter:

a) Dedikerad.

b) Högnivå.

c) Flernivå.

Kapitel II

Definitioner

TILLÄGGSMARKERINGAR

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

15. Med *driftsform för dedikerad säkerhet* avses en driftsform där samtliga personer som har tillgång till systemet har behörighet för uppgifter med den högsta sekretessgrad som hanteras i systemet och för tjänsteutövningen har behov att få tillgång till alla uppgifter som hanteras i systemet.

Anmärkningar:

1. Den allmänna behörigheten att få tillgång till uppgifterna för tjänsteutövningen anger att det inte finns något obligatoriskt krav på datasäkerhetsegenskaper som medger separering av uppgifter i systemet.

2. Andra säkerhetsegenskaper (t.ex. fysiska och i förhållande till personal och förfaranden) skall överensstämma med kraven för den högsta sekretessgraden och samtliga kategoribeteckningar för de uppgifter som hanteras i systemet.

16. Med *driftsform för högnivåsäkerhet* avses en driftsform där samtliga personer som har tillgång till systemet har behörighet för uppgifter med den högsta sekretessgraden som hanteras i systemet, men där inte samtliga personer som har tillgång till systemet har allmän behörighet för tjänsteutövningen att få tillgång till de uppgifter som hanteras i systemet.

Anmärkningar:

1. Avsaknaden av allmän behörighet anger att det finns ett krav på datasäkerhetsegenskaper som medger selektiv tillgång till och separering av uppgifter i systemet.

2. Andra säkerhetsegenskaper (t.ex. fysiska och i förhållande till personal och förfaranden) skall överensstämma med kraven för den högsta sekretessgraden och samtliga kategoribeteckningar för de uppgifter som hanteras i systemet.

3. Alla uppgifter som hanteras eller är tillgängliga i ett system med denna driftsform liksom de utdata som genereras, skall skyddas på det sätt som gäller för uppgifter med den högsta kategoribeteckningen och sekretessgraden som hanteras till dess att annat beslutas, såvida inte etikettfunktionen har godtagbar tillförlitlighet.

17. Med *driftsform för flernivåsäkerhet* avses en driftsform där inte samtliga personer som har tillgång till systemet har behörighet för uppgifter med den högsta sekretessgraden som hanteras i systemet och där inte samtliga personer som har tillgång till systemet har allmän behörighet för de uppgifter som hanteras i systemet.

Anmärkningar:

1. Denna driftsform gör det möjligt att obehindrat hantera uppgifter med olika sekretessgrad och olika kategoribeteckning.

2. Det faktum att inte samtliga personer har behörighet för uppgifter med den högsta sekretessgraden samt avsaknaden av allmän behörighet anger att det finns ett krav på datasäkerhetsegenskaper som medger selektiv tillgång till och separering av uppgifter i systemet.

18. Med *informationssäkerhet* avses tillämpning av säkerhetsåtgärder för att skydda uppgifter som bearbetas, lagras eller överförs i kommunikations- och informationssystem och andra elektroniska system mot att sekretess, okränkbarhet eller tillgänglighet oavsiktligt eller avsiktligt går förlorade samt för att förhindra att själva systemens okränkbarhet och tillgänglighet går förlorade. Informationssäkerhetsåtgärder omfattar säkerhetsåtgärder avseende datorer, överföring, sändning och kryptering samt upptäckt, dokumentering och motverkande av hot mot uppgifterna och systemen.

19. Med *datasäkerhet* avses tillämpning av säkerhetsegenskaper för maskinvara, fasta program och programvara i ett datasystem för att skydda mot, eller förhindra, obehörigt röjande och obehörig manipulation och ändring/radering av uppgifter eller funktionsförlust.

20. Med *datasäkerhetsprodukt* avses en generisk datasäkerhetsprodukt som är avsedd att införlivas med ett IT-system för att förbättra eller möjliggöra sekretess, okränkbarhet eller tillgänglighet för de uppgifter som hanteras.

21. Med *kommunikationssäkerhet* avses tillämpning av säkerhetsåtgärder på telekommunikationer så att obehöriga personer inte skall kunna få fram värdefulla uppgifter ur innehav och studium av dessa telekommunikationer, eller så att telekommunikationernas autenticitet garanteras.

Anmärkning:

Dessa åtgärder omfattar krypterings-, överförings- och sändningssäkerhet, säkerhet i förhållande till förfaranden, fysiska egenskaper, personal och handlingar samt datasäkerhet.

22. Med *utvärdering* avses en lämplig myndighets ingående tekniska undersökning av ett systems eller en krypterings- eller datasäkerhetsprodukts säkerhetsaspekter.

Anmärkningar:

1. Vid utvärderingen kontrolleras om de nödvändiga säkerhetsfunktionerna finns och om de saknar negativa effekter samt bedöms om dessa funktioner går att manipulera.

2. Vid utvärderingen avgörs i vilken utsträckning säkerhetskraven för ett system eller säkerhetsmålen för en datasäkerhetsprodukt är uppfyllda samt fastställs systemets eller krypteringens säkerhetsnivå eller datasäkerhetsproduktens tillförlitlighet.

23. Med *certifiering* avses utfärdande av ett formell intyg, som stöds av en oberoende granskning av genomförandet och resultatet av en utvärdering, om i vilken utsträckning ett system uppfyller säkerhetskraven eller en datasäkerhetsprodukt uppfyller de på förhand fastställda säkerhetsmålen.

24. Med *ackreditering* avses tillstånd och godkännande som beviljas ett system att bearbeta sekretessbelagda EU-uppgifter i systemets driftsmiljö.

Anmärkning:

Ackrediteringen bör göras efter det att alla relevanta säkerhetsförfaranden har införts och tillräckligt hög skyddsnivå för systemresurserna har uppnåtts. Ackrediteringen bör normalt göras på grundval av redovisningen av systemspecifika säkerhetskrav och omfatta följande:

a) En redovisning av syftet med ackrediteringen av systemet; särskilt de hanterade uppgifternas sekretessgrader och vilken eller vilka säkra driftsformer som föreslås för systemet eller nätet.

b) En översikt över riskhanteringen för att identifiera hot och sårbarhet samt åtgärder för att motverka dessa.

c) Säkra driftsmetoder med en ingående beskrivning av de föreslagna operationerna (t.ex. de driftsformer och tjänster som skall tillhandahållas) samt en beskrivning av de säkerhetsegenskaper hos systemet som skall ligga till grund för ackrediteringen.

d) En plan för införandet och upprätthållandet av säkerhetsegenskaperna.

e) En plan för inledande och uppföljande testning, utvärdering och certifiering av system- eller nätsäkerhet.

f) I förekommande fall, certifiering tillsammans med andra faktorer i ackrediteringen.

25. Med *IT-system* avses en samling utrustning, metoder och förfaranden och, i förekommande fall, personal och där syftet är att bearbeta uppgifter.

Anmärkningar:

1. Med detta skall avses en samling anordningar som är konfigurerade för att hantera uppgifter i systemet.

2. Sådana system kan stödja tillämpningsprogram för konsultation, ledning och kommunikation samt vetenskapliga och administrativa tillämpningsprogram, bland annat ordbehandling.

3. Gränserna för ett system skall allmänt fastställas som de element som kontrolleras av en enda myndighet för drift av IT-system.

4. Ett IT-system kan innehålla undersystem, varav en del själva kan vara IT-system.

26. Ett IT-systems säkerhetsegenskaper omfattar alla funktioner, karakteristika och egenskaper hos maskinvara/fasta program/programvara; driftsmetoder, ansvarsförfaranden och åtkomstkontroller, IT-område, separata terminaler/arbetsstationer, hanteringskrav, fysisk struktur och fysiska anordningar, de kontroller av personal och kommunikationer som behövs för att uppnå en godtagbar skyddsnivå för sekretessbelagda uppgifter som skall hanteras i ett IT-system.

27. Med *IT-nät* avses en geografiskt utspridd organisation av sammankopplade IT-system för utväxling av data som omfattar de sammankopplade IT-systemens komponenter samt gränssnitt mellan dessa och de stödjande data- eller kommunikationsnäten.

Anmärkningar:

1. Ett IT-nät kan utnyttja tjänsterna från ett eller flera kommunikationsnät för att kopplas samman för utväxling av data; flera IT-nät kan utnyttja tjänsterna från ett gemensamt kommunikationsnät.

2. Ett IT-nät kallas ”lokalt” om det kopplar samman flera datorer på samma plats.

28. Ett IT-näts säkerhetsegenskaper omfattar säkerhetsegenskaperna hos de enskilda IT-system som ingår i nätet tillsammans med de ytterligare komponenter och egenskaper som hör ihop med själva nätet (t.ex. nätkommunikation, mekanismer och förfaranden för säkerhetsidentifikation och säkerhetsetiketter, åtkomstkontroller, program och identifikation) och som behövs för att tillhandahålla en godtagbar skyddsnivå för sekretessbelagda uppgifter.

29. Med *IT-utrymme* avses ett utrymme som innehåller en eller flera datorer, deras lokala kringutrustning och lagringsenheter samt specialiserad nät- och kommunikationsutrustning.

Anmärkning:

Detta omfattar inte ett separat utrymme där kringutrustning eller terminaler/arbetsstationer är belägna även om dessa är sammankopplade med utrustning i IT-utrymmet.

30. Med *separat utrymme med terminaler/arbetsstationer* avses ett utrymme som är skilt från ett IT-utrymme och som innehåller viss datorutrustning, lokal kringutrustning eller terminaler/arbetsstationer och eventuell tillhörande kommunikationsutrustning.

31. Med *Tempest-motåtgärder* avses säkerhetsåtgärder som är avsedda att skydda utrustning och kommunikationsinfrastruktur mot att sekretessbelagda uppgifter röjs genom oavsiktlig elektromagnetisk strålning.

Kapitel III

Ansvar för säkerhet

ALLMÄNT

32. Den säkerhetskommitté som definieras i avsnitt 1 punkt 4 skall också ha ansvar för frågor om informationssäkerhet. Säkerhetskommittén skall organisera sitt arbete så att den kan avge expertutlåtanden om dessa frågor.

33. Om det uppstår problem när det gäller säkerheten (incidenter, överträdelser osv.) skall den ansvariga nationella myndigheten och/eller generalsekretariatets säkerhetsavdelning omedelbart vidta åtgärder. Alla problem skall hänskjutas till generalsekretariatets säkerhetsavdelning.

34. Generalsekreteraren/den höge representanten eller, i förekommande fall, chefen för en decentraliserad EU-myndighet skall inrätta en avdelning för informationssäkerhet som skall ge riktlinjer till säkerhetsmyndigheten för införande och kontroll av särskilda säkerhetsegenskaper som ingår i systemen.

ACKREDITERINGSMYNDIGHET FÖR SÄKERHET

35. Ackrediteringsmyndigheten för säkerhet skall vara

— en nationell säkerhetsmyndighet,

— den myndighet som har utsetts av generalsekreteraren/den höge representanten,

— säkerhetsmyndigheten vid en decentraliserad EU-myndighet, eller

— deras bemyndigade/utsedda företrädare, beroende på vilket system som skall ackrediteras.

36. Ackrediteringsmyndigheten för säkerhet skall ansvara för att systemen överensstämmer med rådets säkerhetsstrategi. En av dess uppgifter skall vara att godkänna system för hantering i driftsmiljön av sekretessbelagda EU-uppgifter upp till en fastställd sekretessgrad. När det gäller generalsekretariatet och, i förekommande fall, decentraliserade EU-myndigheter skall ackrediteringsmyndigheten för säkerhet ansvara för säkerheten för generalsekreterarens/den höge representantens eller den decentraliserade myndighetens chefs räkning.

Behörigheten för ackrediteringsmyndigheten för säkerhet vid generalsekretariatet skall omfatta alla system som är i drift i generalsekretariatets byggnader. System och systemkomponenter som är i drift i en medlemsstat skall fortfarande omfattas av den medlemsstatens behörighet. Om en del komponenter i ett system omfattas av behörigheten för ackrediteringsmyndigheten för säkerhet vid generalsekretariatet och andra komponenter omfattas av behörigheten för andra ackrediteringsmyndigheter för säkerhet, skall samtliga parter utse en gemensam ackrediteringsstyrelse som skall samordnas av ackrediteringsmyndigheten för säkerhet vid generalsekretariatet.

MYNDIGHET FÖR INFORMATIONSSÄKERHET

37. Myndigheten för informationssäkerhet skall ansvara för verksamheten avseende informationssäkerhet. När det gäller generalsekretariatet och, i förekommande fall, decentraliserade EU-myndigheter skall myndigheten för informationssäkerhet ansvara för att

— ge tekniska utlåtanden och tekniskt bistånd till ackrediteringsmyndigheten för säkerhet,

— bistå vid utarbetandet av redovisningar av systemspecifika säkerhetskrav,

— granska redovisningar av systemspecifika säkerhetskrav för att säkerställa att de överensstämmer med de här säkerhetsbestämmelserna, strategin för informationssäkerhet och dokument om säkerhetsarkitektur,

— delta i ackrediteringspanelerna/-styrelserna vid behov och i samband med ackrediteringar ge rekommendationer om informationssäkerhet till ackrediteringsmyndigheten för säkerhet,

— stödja utbildning om informationssäkerhet,

— avge tekniska utlåtanden vid utredningar om informationssäkerhetsrelaterade incidenter,

— fastställa tekniska strategiska riktlinjer för att säkerställa att endast godkänd programvara används.

MYNDIGHET FÖR DRIFT AV IT-SYSTEM

38. Myndigheten för informationssäkerhet skall så tidigt som möjligt delegera ansvaret för genomförandet och kontrollerna samt för särskilda säkerhetsegenskaper till myndigheten för drift av IT-system. Detta ansvar skall gälla under systemets hela livscykel, från projektplaneringsstadiet till det slutliga bortskaffandet.

39. Myndigheten för drift av IT-system skall ansvara för alla säkerhetsåtgärder som ingår i det samlade systemet. Ansvaret omfattar utarbetande av säkra driftsmetoder. Myndigheten för drift av IT-system skall specificera vilka säkerhetsnormer och säkerhetsrutiner som systemets leverantör skall följa.

40. Myndigheten för drift av IT-system får delegera en del av sitt ansvar när så är lämpligt, t.ex. till tjänstemannen för informationssäkerhet och tjänstemannen för informationssäkerhet på plats. De olika informationssäkerhetsuppgifterna får utföras av en enda person.

ANVÄNDARE

41. Alla användare skall ansvara för att deras handlingar inte inverkar negativt på säkerheten i det system de använder.

UTBILDNING OM INFORMATIONSSÄKERHET

42. Utbildning om informationssäkerhet skall vid behov ges på olika nivåer och för olika kategorier av personal inom generalsekretariatet, decentraliserade EU-myndigheter eller ministerier i medlemsstaterna.

Kapitel IV

Icke-tekniska säkerhetsåtgärder

PERSONALSÄKERHET

43. Användarna av systemet skall genomgå säkerhetsprövning och ha behov av uppgifterna för sin tjänsteutövning, i förekommande fall, för uppgifter av den sekretessgrad och med det innehåll som hanteras i deras särskilda system. Tillgång till viss utrustning eller information som är specifik för systemens säkerhet kommer att kräva särskild behörighet som skall utfärdas i enlighet med rådets förfaranden.

44. Ackrediteringsmyndigheten för säkerhet skall ange alla känsliga befattningar och specificera vilken säkerhetsprövning och övervakning som krävs för all personal som innehar dem.

45. Systemen skall specificeras och utformas så att fördelningen av uppgifter och ansvar till personalen underlättas för att förhindra att en person har fullständig kännedom om eller kontroll över de viktiga punkterna i systemets säkerhet. Målet bör vara att det skall krävas att två eller flera personer står i maskopi med varandra för att systemet eller nätet avsiktligt skall kunna ändras eller förstöras.

FYSISK SÄKERHET

46. IT-utrymmen och separata utrymmen med terminaler/arbetsstationer (enligt definitionerna i punkterna 29 och 30) där EU-uppgifter med sekretessgraden CONFIDENTIEL UE och högre hanteras med hjälp av informationsteknik eller där åtkomst till sådana uppgifter är möjlig, skall fastställas som EU-säkerhetsutrymme av klass I eller klass II eller, i förekommande fall, den nationella motsvarigheten.

47. På IT-utrymmen och separata utrymmen med terminaler/arbetsstationer där systemets säkerhet kan ändras måste mer än en behörig tjänsteman/annan anställd samtidigt vara på plats.

KONTROLL AV ÅTKOMST TILL ETT SYSTEM

48. All information och materiel som möjliggör kontroll av åtkomst till ett system skall skyddas genom åtgärder som motsvarar den högsta sekretessgraden och kategoriberäkningen för de uppgifter som den kan ge tillgång till.

49. När information och materiel för kontroll av åtkomst inte längre används för detta ändamål skall den förstöras i enlighet med punkterna 61–63.

Kapitel V

Tekniska säkerhetsåtgärder

INFORMATIONSSÄKERHET

50. Det skall åligga upphovsmannen till uppgifterna att identifiera och sekretessbelägga alla informationsbärande handlingar, oavsett om de är i form av papperskopior eller lagringsmedier för datorer. På papperskopior skall sekretessgraden anges upptill och nertill på varje sida. Utdata i form av antingen papperskopior eller lagringsmedier för datorer skall ha den sekretessgrad som motsvarar den högsta sekretessgraden för de uppgifter som har använts för att framställa dem. Ett systems driftsform kan också inverka på sekretessgraden för utdata i systemet.

51. Det skall åligga en organisation och de personer i den som innehar information att beakta problemen i samband med aggregering av enskilda uppgifter och de slutsatser som kan dras av sammanhörande delar och avgöra om den samlade informationen bör ges en högre sekretessgrad eller inte.

52. Det faktum att uppgifter kan föreligga i kortkod, överföringskod eller någon form av binär representation ger inte något säkerhetsskydd och bör därför inte påverka uppgifternas sekretessgrad.

53. När uppgifter överförs från ett system till ett annat skall uppgifterna skyddas under överföringen och i det mottagande systemet på ett sätt som motsvarar den ursprungliga sekretessgraden och uppgiftskategorin.

54. Alla lagringsmedier för datorer skall hanteras på ett sätt som motsvarar de lagrade uppgifternas högsta sekretessgrad eller medieetiketten, och de skall alltid skyddas på tillfredsställande sätt.

55. Återanvändningsbara lagringsmedier för datorer som används för sekretessbelagda EU-uppgifter skall behålla den högsta sekretessgrad för vilken de använts till dess att uppgifterna på korrekt sätt har inplacerats i lägre sekretessgrad eller sekretessen har hävts och mediernas sekretessgrad har ändrats i enlighet med detta, deras sekretess har hävts eller de har förstörts genom en metod som godkänts av generalsekretariatet eller på nationell nivå (se punkterna 61–63).

KONTROLL OCH SPÅRBARHET AV UPPGIFTER

56. Automatiska (identifikation) eller manuella loggar/diarier skall föras över tillgång till EU-uppgifter med sekretessgraderna SECRET UE och högre. Dessa register skall bevaras i enlighet med de här säkerhetsbestämmelserna.

57. Sekretessbelagda EU-utdata som förvaras inom IT-utrymmet får hanteras som ett enda sekretessbelagt material och behöver inte registreras, under förutsättning att materialet är identifierat, märkt med sekretessgrad och kontrollerat på lämpligt sätt.

58. När utdata genereras från ett system som hanterar sekretessbelagda EU-uppgifter och från ett IT-utrymme överförs till ett separat utrymme med terminaler/arbetsstationer, skall förfaranden som godkänts av ackrediteringsmyndigheten för säkerhet fastställas för kontroll av fjärrutdata. För EU-uppgifter med sekretessgraden SECRET UE och högre skall sådana förfaranden omfatta särskilda anvisningar för uppgifternas spårbarhet.

HANTERING OCH KONTROLL AV FLYTTBARA LAGRINGSMEDIER FÖR DATORER

59. Alla flyttbara lagringsmedier för datorer med sekretessgraden CONFIDENTIEL UE och högre skall hanteras som materiel och allmänna bestämmelser skall tillämpas. Identifikation och sekretessgrad skall anges på lämpligt sätt med hänsyn till mediets särskilda fysiska utseende så att det tydligt kan kännas igen.

60. Användarna skall ansvara för att se till att sekretessbelagda EU-uppgifter lagras på medier som på lämpligt sätt märks med sekretessgrad och skyddas. Förfaranden skall fastställas för att se till att lagring av alla nivåer av EU-uppgifter på lagringsmedier för datorer görs i enlighet med de här säkerhetsbestämmelserna.

HÄVANDE AV SEKRETESS OCH FÖRSTÖRING AV LAGRINGSMEDIER FÖR DATORER

61. Lagringsmedier för datorer som använts för sekretessbelagda EU-uppgifter får inplaceras i lägre sekretessgrad eller kan få sekretessen hävd om ett förfarande som godkänts av generalsekretariatet eller på nationell nivå används.

62. Lagringsmedier för datorer som har innehållit EU-uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET eller uppgifter av en särskild kategori får inte inplaceras i en lägre sekretessgrad eller få sekretessen hävd och återanvändas.

63. Om sekretessen inte kan hävas för lagringsmedier för datorer eller de inte är återanvändningsbara, skall de förstöras med hjälp av en metod som godkänts av generalsekretariatet eller på nationell nivå.

KOMMUNIKATIONSSÄKERHET

64. När sekretessbelagda EU-uppgifter överförs på elektromagnetisk väg skall särskilda åtgärder vidtas för att skydda dessa överföringars sekretess, okränkbarhet och tillgänglighet. Ackrediteringsmyndigheten för säkerhet skall fastställa kraven för att skydda överföringarna från upptäckt och avlyssning. De uppgifter som överförs i ett kommunikationssystem skall skyddas på grundval av kraven på sekretess, okränkbarhet och tillgänglighet.

65. Om det krävs krypteringsmetoder för att skydda sekretessen, okränkbarheten och tillgängligheten skall sådana metoder eller tillhörande produkter särskilt godkännas för detta ändamål av ackrediteringsmyndigheten för säkerhet.

66. Sekretessen för EU-uppgifter med sekretessgraden SECRET UE och högre skall under överföringen skyddas genom krypteringsmetoder eller krypteringsprodukter som har godkänts av rådet på rekommendation av rådets säkerhetskommitté. Sekretessen för EU-uppgifter med sekretessgraden CONFIDENTIEL UE eller RESTREINT UE skall under överföringen skyddas genom krypteringsmetoder eller med hjälp av krypteringsprodukter som har godkänts antingen av generalsekreteraren/den höge representanten på rekommendation av rådets säkerhetskommitté eller av en medlemsstat.

67. Närmare föreskrifter för överföring av sekretessbelagda EU-uppgifter skall anges i särskilda säkerhetsanvisningar som har godkänts av rådet på rekommendation av rådets säkerhetskommitté.

68. Under exceptionella operativa omständigheter får EU-uppgifter med sekretessgraderna RESTREINT UE, CONFIDENTIEL UE och SECRET UE överföras i klartext under förutsättning att varje tillfälle är uttryckligen godkänt. Sådana exceptionella omständigheter är följande:

a) Vid överhängande eller faktisk kris-, konflikt- eller krigssituation.

b) När en snabb överföring är av största vikt och krypteringsmöjligheter inte är tillgängliga, och det bedöms att de överförda uppgifterna inte kan utnyttjas i tid för att skada operationerna.

69. Ett system skall ha förmåga att uttryckligen vägra tillgång till sekretessbelagda EU-uppgifter vid någon eller alla av dess separata arbetsstationer eller terminaler när detta krävs, antingen genom fysisk frånkoppling eller genom särskilda egenskaper hos programvaran som har godkänts av ackrediteringsmyndigheten för säkerhet.

INSTALLATIONS- OCH STRÅLNINGSSÄKERHET

70. Den ursprungliga installationen av system och eventuella större ändringar av dem skall utföras av installatörer som har genomgått säkerhetsprövning, under ständig övervakning av tekniskt kunnig personal som har behörighet för tillgång till sekretessbelagda EU-uppgifter upp till den nivå som motsvarar den högsta sekretessgraden för de uppgifter som systemet förväntas lagra och hantera.

71. All utrustning skall installeras i enlighet med rådets gällande säkerhetsstrategi.

72. System i vilka EU-uppgifter med sekretessgraden CONFIDENTIEL UE och högre hanteras skall skyddas så att deras säkerhet inte kan hotas av sådan kompromettерande strålning vars studium och kontroll betecknas ”Tempest”.

73. Tempest-motåtgärder för installationer vid generalsekretariatet och decentraliserade EU-myndigheter skall granskas och godkännas av en Tempest-myndighet som utsetts av säkerhetsmyndigheten vid generalsekretariatet. För nationella installationer i vilka sekretessbelagda EU-uppgifter hanteras skall tillståndsmyndigheten vara den erkända nationella Tempest-tillståndsmyndigheten.

Kapitel VI

Säkerhet under hantering

SÄKRA DRIFTSMETODER

74. I de säkra driftsmetoderna fastställs principerna för säkerhetsfrågor, vilka driftsmetoder som skall användas samt personalens ansvar. Myndigheten för drift av IT-system skall ansvara för utarbetandet av säkra driftsmetoder.

SKYDD FÖR PROGRAMVARA/KONFIGURERINGSHANTERING

75. Säkerhetsskyddet för tillämpningsprogram skall fastställas på grundval av en bedömning av själva programmets sekretessgrad snarare än på grundval av sekretessgraden av de uppgifter som det skall bearbeta. De programvaruversioner som används bör kontrolleras med regelbundna mellanrum så att deras okränkbarhet säkerställs och att de fungerar korrekt.

76. Nya eller ändrade versioner av programvara bör inte användas för att hantera sekretessbelagda EU-uppgifter förrän de har kontrollerats av myndigheten för drift av IT-system.

KONTROLL AV FÖREKOMST AV SKADLIGA PROGRAMVARU- ELLER DATAVIRUS

77. Kontroll av förekomst av skadliga programvaru- eller datavirus skall utföras regelbundet i enlighet med kraven från ackrediteringsmyndigheten för säkerhet.

78. Alla lagringsmedier för datorer som kommer till generalsekretariatet, decentraliserade EU-myndigheter eller medlemsstaterna bör kontrolleras med avseende på eventuella skadliga programvaru- eller datavirus innan de börjar användas i ett system.

UNDERHÅLL

79. Kontrakt och metoder för regelbundet underhåll och jourunderhåll av system, för vilka en redovisning av systemspecifika säkerhetskrav har utarbetats, skall innehålla krav och arrangemang för den underhållspersonal och deras utrustning som kommer in i ett IT-utrymme.

80. Kraven skall klart anges i redovisningen av systemspecifika säkerhetskrav och metoderna skall klart anges i de säkra driftsmetoderna. Kontrakterat underhåll som kräver diagnosmetoder med åtkomst på avstånd skall endast tillåtas i undantagsfall, under strikt säkerhetskontroll, och endast med godkännande från ackrediteringsmyndigheten för säkerhet.

Kapitel VII

Upphandling

81. Alla säkerhetsprodukter som skall användas i systemet och som skall upphandlas bör antingen ha utvärderats och certifierats eller hålla på att utvärderas och certifieras av ett lämpligt utvärderings- eller certifieringsorgan på grundval av internationellt erkända kriterier (t.ex. de gemensamma kriterierna för utvärdering av informationsteknisk säkerhet, ISO 15408).

82. I samband med beslut om utrustning, särskilt lagringsmedier för datorer, bör hyras i stället för köpas måste det beaktas dels att när sådan utrustning har använts för att hantera sekretessbelagda EU-uppgifter kan den inte släppas utanför en tillräckligt säker miljö utan att ackrediteringsmyndigheten för säkerhet har gett tillstånd till att sekretessen hävs, dels att ett sådant tillstånd kanske inte alltid kan erhållas.

ACKREDITERING

83. Alla system för vilka en redovisning av systemspecifika säkerhetskrav skall utarbetas innan sekretessbelagda EU-uppgifter hanteras, skall ackrediteras av ackrediteringsmyndigheten för säkerhet på grundval av information i redovisningen av systemspecifika säkerhetskrav, säkra driftsmetoder och annan relevant dokumentation. Undersystem och separata terminaler/arbetsstationer skall ackrediteras som en del av alla de system som de är kopplade till. Om ett system utnyttjas av såväl rådet som andra organisationer skall generalsekretariatet och de relevanta säkerhetsmyndigheterna inbördes komma överens om ackrediteringen.

84. Ackrediteringsförfarandet kan utföras i enlighet med en ackrediteringsstrategi som är lämpad för det särskilda systemet och fastställd av ackrediteringsmyndigheten för säkerhet.

UTVÄRDERING OCH CERTIFIERING

85. Före ackrediteringen skall det i vissa fall utvärderas och certifieras att säkerhetsegenskaperna hos maskinvara, fasta program och programvara i ett system har förmåga att skydda uppgifter på den avsedda sekretessnivån.

86. Kraven för utvärdering och certifiering skall ingå i systemplaneringen och klart anges i redovisningen av systemspecifika säkerhetskrav.

87. Utvärderings- och certifieringsförfarandena skall utföras i enlighet med godkända riktlinjer av personal som är tekniskt kunnig och har genomgått lämplig säkerhetsprövning och som agerar för myndigheten för drift av IT-system.

88. Grupperna kan tillhandahållas från en utsedd medlemsstats utvärderings- eller certifieringsmyndighet eller deras utsedda företrädare, t.ex. en kunnig leverantör som genomgått säkerhetsprövning.

89. Utvärderings- och certifieringsförfarandena kan vara mindre omfattande (t.ex. endast omfatta integreringsaspekter) om systemen bygger på befintliga nationellt utvärderade och certifierade datasäkerhetsprodukter.

RUTINKONTROLL AV SÄKERHETSEGENSKAPER FÖR FORTSATT ACKREDITERING

90. Myndigheten för drift av IT-system skall fastställa förfaranden för rutinkontroll för att säkerställa att systemets alla säkerhetsegenskaper är fortsatt giltiga.

91. De typer av förändringar som föranleder ny ackreditering eller förhandstillstånd från ackrediteringsmyndigheten för säkerhet skall klart fastställas och anges i redovisningen av systemspecifika säkerhetskrav. Efter varje ändring, reparation eller fel som kan ha påverkat systemets säkerhetsegenskaper skall myndigheten för drift av IT-system se till att en kontroll utförs för att säkerställa att säkerhetsegenskaperna fungerar korrekt. Fortsatt ackreditering av systemet skall normalt vara avhängig av att dessa kontroller har genomförts med tillfredsställande resultat.

92. Alla system där säkerhetsegenskaper har införts skall regelbundet inspekteras eller granskas av ackrediteringsmyndigheten för säkerhet. För system i vilka EU-uppgifter med sekretessgraden TRÈS SECRET UE/EU TOP SECRET eller med tilläggsmarkeringar hanteras skall inspektionerna genomföras minst en gång per år.

Kapitel VIII

Tillfällig eller sporadisk användning

SÄKERHET FÖR MIKRODATORER/PERSONDATORER

93. Mikrodatorer/persondatorer med fasta skivminnen (eller andra beständiga lagringsmedier) som fungerar antingen fristående eller som nätfigurationer samt bärbar datorutrustning (t.ex. bärbara persondatorer och andra bärbara datorer) med fasta hårddiskar skall betraktas som informationslagringsmedier i samma mening som disketter eller andra flyttbara lagringsmedier för datorer.

94. Denna utrustning skall ges den skyddsnivå i fråga om åtkomst, hantering, lagring och transport som motsvarar den högsta sekretessgraden för de uppgifter som vid något tillfälle lagras och bearbetas (till dess att den inplaceras i lägre sekretessgrad eller sekretessen hävs genom godkända förfaranden).

ANVÄNDNING AV PRIVATÄGD IT-UTRUSTNING FÖR OFFICIELLT RÅDSARBETE

95. Det skall vara förbjudet att använda privatägda flyttbara lagringsmedier för datorer och privatägd programvara och maskinvara (t.ex. persondatorer och bärbara datorer) för att hantera sekretessbelagda EU-uppgifter.

96. Privatägd maskinvara och programvara och privatägda lagringsmedier får inte föras in till något utrymme i klass I eller II, där sekretessbelagda EU-uppgifter hanteras, utan tillstånd från chefen för säkerhetsavdelningen vid generalsekretariatet, chefen för en medlemsstats ministerium respektive chefen för en decentraliserad EU-myndighet.

ANVÄNDNING AV LEVERANTÖRSÄGD ELLER NATIONELLT TILLHANDAHÅLLEN IT-UTRUSTNING FÖR OFFICIELLT RÅDSARBETE

97. Chefen för säkerhetsavdelningen vid generalsekretariatet, chefen för en medlemsstats ministerium respektive chefen för en decentraliserad EU-myndighet kan tillåta att leverantörsägd IT-utrustning och programvara används i organisationer som stöd för officiellt rådsarbete. Det kan också vara tillåtet för anställda vid generalsekretariatet eller en decentraliserad EU-myndighet att använda nationellt tillhandahållen IT-utrustning och programvara; i detta fall skall IT-utrustningen sättas upp på inventarieförteckningen som hålls vid generalsekretariatet. Om IT-utrustningen skall användas för att hantera sekretessbelagda EU-uppgifter skall i båda fallen den lämpliga ackrediteringsmyndigheten för säkerhet konsulteras så att de inslag i informationssäkerheten som är tillämpliga på användningen av denna utrustning beaktas och genomförs på korrekt sätt.

AVSNITT XII

UTLÄMNANDE AV SEKRETESSBELAGDA EU-UPPGIFTER TILL TREDJE LAND ELLER INTERNATIONELLA ORGANISATIONER

PRINCIPER FÖR UTLÄMNANDE AV SEKRETESSBELAGDA EU-UPPGIFTER

1. Beslut om att lämna ut sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer skall fattas av rådet på grundval av

   — typen av och innehållet i sådana uppgifter,

   — mottagarens behov av uppgifterna för sin tjänsteutövning,

   — omfattningen av fördelarna för EU.

   Den medlemsstat som är upphovsman till de sekretessbelagda EU-uppgifter som skall lämnas ut skall tillfrågas om sitt samtycke.

2. Dessa beslut skall fattas från fall till fall och vara avhängiga av

   — den önskade graden av samarbete med berört tredje land eller berörda internationella organisationer,

   — den tilltro som kan sättas till dem – vilket följer av den säkerhetsnivå som skulle tillämpas på de sekretessbelagda EU-uppgifter som anförtros dessa stater eller organisationer, och av överensstämmelsen mellan de säkerhetsbestämmelser som tillämpas där och de som tillämpas i EU. Rådets säkerhetskommitté skall avge ett tekniskt yttrande till rådet i denna fråga.

3. Om tredje land eller internationella organisationer godtar sekretessbelagda EU-uppgifter skall detta innebära en garanti för att uppgifterna inte kommer att användas för andra syften än dem som var anledningen till att uppgifterna lämnades ut eller utväxlades, och att tillhandahållandet av det skydd som rådet kräver garanteras.

NIVÅER

4. När rådet har beslutat att sekretessbelagda uppgifter får lämnas ut eller utväxlas med en given stat eller internationell organisation, skall det besluta om vilken samarbetsnivå som är möjlig. Detta skall i synnerhet vara avhängigt av den säkerhetspolitik och de säkerhetsbestämmelser som den staten eller organisationen tillämpar.

5. Följande tre samarbetsnivåer är möjliga:

   Nivå 1

   Samarbete med tredje land eller med internationella organisationer vilkas säkerhetspolitik och säkerhetsbestämmelser ligger mycket nära EU:s.

   Nivå 2

   Samarbete med tredje land eller med internationella organisationer vilkas säkerhetspolitik och säkerhetsbestämmelser märkbart skiljer sig från EU:s.

   Nivå 3

   Tillfälligt samarbete med tredje land eller med internationella organisationer vilkas politik och säkerhetsbestämmelser inte kan bedömas.

6. På varje samarbetsnivå skall det beslutas om vilka säkerhetsbestämmelser, omformulerade i enskilda fall mot bakgrund av det tekniska yttrandet från rådets säkerhetskommitté, som mottagarna skall anmodas att tillämpa på skyddet av de sekretessbelagda uppgifter som lämnas ut till dem. Dessa förfaranden och säkerhetsbestämmelser beskrivs i tillägg 4, 5 och 6.

AVTALEN

7. När rådet har beslutat att det föreligger ett ständigt eller långsiktigt behov av att utväxla sekretessbelagda uppgifter mellan EU och tredje land eller andra internationella organisationer, skall det utforma ”avtal om säkerhetsförfaranden för utväxling av sekretessbelagda uppgifter” med dem och i dessa skall syftet med samarbetet samt de ömsesidiga bestämmelserna om skyddet av de uppgifter som utväxlas fastställas.

8. När det gäller nivå 3 om tillfälligt samarbete som per definition är begränsat i tiden och till syftet, får ”avtalet om säkerhetsförfaranden för utväxling av sekretessbelagda uppgifter” ersättas av ett enkelt samförståndsavtal i vilket det fastställs vilken typ av sekretessbelagda uppgifter som skall utväxlas samt de ömsesidiga skyldigheterna beträffande dessa uppgifter, under förutsättning att de är klassificerade som RESTREINT UE eller lägre.

9. Utkast till avtal om säkerhetsförfaranden eller samförståndsavtal skall godkännas av säkerhetskommittén innan de läggs fram för rådet för beslut.

10. Nationella säkerhetsmyndigheter skall bistå generalsekreteraren/den höge representanten på alla de sätt som är nödvändiga för att säkerställa att de uppgifter som skall lämnas ut används och skyddas i enlighet med bestämmelserna i avtalen om säkerhetsförfaranden eller samförståndsavtalen.

Tillägg 1

Förteckning över nationella säkerhetsmyndigheter

BELGIEN

Ministère des Affaires Etrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Telefon: 32-2-501 85 14
Fax: 32-2-501 80 58
Telex: 21376
Telegramadress: Direction de Sécurité A01 — MINAFET

DANMARK

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefon: 45 33 14 88 88
Fax: 45 38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø.
Telefon: 45 33 32 55 66
Fax: 45 33 93 13 20

TYSKLAND

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefon: 49-30-39 81 15 28
Fax: 49-30-39 81 16 10

GREKLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετράωρο)
Φαξ: 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos — Athens
Greece
Telefon: 00 30-1-655 22 03 (kontorstid)
00 30-1-655 22 05 (dygnet runt)
Fax: 00 30-1-642 69 40

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
Telefon: 34-91-372 57 07
Fax: 34-91-372 58 08
E-mail: nsa-sp@areatec.com

FRANKRIKE

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefon: 33-0-144 18 81 80
Fax: 33-0-144 18 82 00
Telex: SEGEDEFNAT 200019
Telegramadress: SEGEDEFNAT PARIS

IRLAND

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefon: 353-1-478 08 22
Fax: 353-1-478 14 84

ITALIEN

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefon: 39-06-627 47 75
Fax: 39-06-614 33 97
Telex: 623876 AQUILA 1
Telegramadress: ess: PCM-ANS-UCSI-ROMA

LUXEMBURG

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L-1023 Luxembourg
Telefon: 352-478 22 10 central
352-478 22 35 direct
Fax: 352-478 22 43
352-478 22 71
Telex: 3481 SERET LU
Telegramadress: MIN D'ETAT — ANS

NEDERLÄNDERNA

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefon: 31-70-320 44 00
Fax: 31-70-320 07 33
Telex: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
Telefon: 31-70-318 70 60
Fax: 31-70-318 79 51

ÖSTERRIKE

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefon: 43-1-531 15 34 64
Fax: 43-1-531 8 52 19

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefon: 351-21-301 55 10
351-21-301 00 01, ank. 20 45 37
Fax: 351-21-302 03 50

FINLAND

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefon: 358-9-13 41 53 38
Fax: 358-9-13 41 53 03

SVERIGE

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon: 46-8-405 54 44
Fax: 46-8-723 11 76

FÖRENADE KUNGARIKET

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1 AH
Telefon: 44-20-72 70 87 51
Fax: 44-20-76 30 14 28
Telegramadress: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Tillägg 2

Jämförelse av nationella sekretessgrader

EU-sekretessregler	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
NATO classification ([1])				
WEU classification	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Belgien	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	STRENG GEHEIM	GEHEIM	VS ([2]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grekland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spanien	Secreto	Reservado	Confidencial	Difusion Limitada
Frankrike	Très Secret Défense ([3])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Nederländerna	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sverige	Kvalificerat hemlig	Hemligt	Hemligt	Hemligt
Förenade kungariket	Top Secret	Secret	Confidential	Restricted

([1]) Nato: Överensstämmelsen med Natos sekretessgrader kommer att fastställas vid förhandlingarna om säkerhetsavtalet mellan Europeiska unionen och Nato.
([2]) Tyskland: VS = Verschlusssache.
([3]) Frankrike: Sekretessgraden "Très Secret Défense" omfattar regeringens prioriteringar och får endast ändras med premiärministerns tillåtelse.

Tillägg 3

Praktisk handledning om säkerhetsklassning

Denna handledning är vägledande och får inte tolkas på så sätt att den innebär ändringar av de väsentliga bestämmelserna i avsnitten II och III.

Säkerhetsklassning	När	Vem	Markeringar	Inplacering i en lägre sekretessgrad/hävande av sekretessen/förstöring	
				Vem	När
TRÈS SECRET UE/EU TOP SECRET (kvalificerat hemligt): denna sekretessgrad skall endast användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen synnerligen allvarlig skada (synnerligt men). [Avsnitt II.1].	Att röja uppgifter med beteckningen TRÈS SECRET UE/EU TOP SECRET kan: — utgöra ett direkt hot mot EU:s eller någon av dess medlemsstaters eller vänligt sinnade länders inre stabilitet, — vålla synnerligen allvarlig skada på förbindelserna med vänligt sinnade regeringar, — direkt leda till omfattande förlust av liv, — vålla synnerligen allvarlig skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters styrkor eller på ytterst värdefulla säkerhets- eller underrättelseoperationer, — vålla allvarlig långsiktig skada på EU:s eller medlemsstaternas ekonomi.	Medlemsstaterna: Vederbörligen behöriga personer (upphovsmannen) [Avsnitt III.4]. Generalsekretariatet: Vederbörligen behöriga personer (upphovsmannen) [Avsnitt III.4], generalsekreteraren/den höge representanten och ställföreträdande generalsekreteraren. Upphovsmannen skall ange ett datum eller en tidsperiod när uppgifterna får inplaceras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall skall upphovsmannen se över handlingarna minst vart femte år för att säkerställa att den ursprungliga säkerhetsklassningen fortfarande är nödvändig [Avsnitt III.10].	Sekretessgraden TRÈS SECRET UE/EU TOP SECRET skall användas för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET och, om detta är tillämpligt, förses med ESDP/PESD-märkning på mekanisk väg eller för hand [Avsnitt II.8]. EU: sekretessgrad skall anges centrerat i marginalen upptill och nedtill på varje sida, och varje sida skall numreras. På varje handling skall ett referensnummer och ett datum anges. Referensnumret skall anges på varje sida. Om flera kopior skall lämnas ut skall ett kopienummer anges på första sidan på varje exemplar, tillsammans med en uppgift om det totala antalet sidor. På första sidan skall det finnas en förteckning över alla bilagor och bifogade handlingar [Avsnitt VII.1].	Beslut om hävande av sekretessen eller inplacering i en lägre sekretessgrad får endast fattas av upphovsmannen, eller generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren som skall informera eventuella efterföljande mottagare till vilka de har lämnat ut eller kopierat handlingen om förändringen [Avsnitt III.9]. Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET skall förstöras av det centrala registret eller den underavdelning till det centrala registret som är ansvarigt för dem. Varje förstörd handling skall förtecknas i ett intyg över förstöring som skall undertecknas av den kontrolltjänstemannen för beteckningen TRÈS SECRET UE/EU TOP SECRET och av den tjänsteman som bevittnar förstöringen. Dessa personer skall ha genomgått säkerhetsprövning för sekretessgraden TRÈS SECRET UE/EU TOP SECRET. En notering om detta skall göras i registret. Registret skall bevara intygen om förstöring tillsammans med distributionslistan under tio år [Avsnitt VII.31].	Överskottskopior och handlingar som inte längre behövs måste förstöras [Avsnitt VII.31]. Handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, inklusive allt sekretessbelagt material som skall förstöras och som är resultatet av upprättandet av handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET, till exempel dåliga kopior, arbetsutkast, maskinskrivna noter och karbonpapper, skall förstöras under överinseende av en tjänsteman med graden TRÈS SECRET UE/EU TOP SECRET genom att brännas, omvandlas till pappersmassa, gå igenom en dokumentförstörare eller på annat sätt reduceras så att de är oigenkännliga och icke möjliga att återställa [Avsnitt VII.31c].

Säkerhetsklassning	När	Vem	Markeringar	Inplacering i en lägre sekretessgrad/hävande av sekretessen/förstöring	
				Vem	När
SECRET UE (hemligt): denna sekretessgrad skall endast användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen allvarlig skada (icke obetydligt men). [Avsnitt II.2].	Att röja uppgifter med beteckningen SECRET UE kan: — skapa internationella spänningar, — allvarligt skada förbindelserna med vänligt sinnade regeringar, — utgöra ett direkt hot mot liv eller allvarligt skada den allmänna ordningen eller den enskildes säkerhet eller frihet, — vålla allvarlig skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters styrkor, eller på den fortsatta effektiviteten hos ytterst värdefulla säkerhets- eller underrättelseoperationer, — vålla väsentlig materiell skada på EU:s eller en av dess medlemsstaters finansiella, monetära, ekonomiska och kommersiella intressen.	Medlemsstaterna: Befullmäktigade personer (upphovsmannen) [Avsnitt III.2]. Generalsekretariatet och EU:s decentraliserade organ: Behöriga personer (upphovsmannen) [Avsnitt III.2], generaldirektörer, generalsekreteraren/den höge representanten och ställföreträdande generalsekreteraren. Upphovsmannen skall ange ett datum eller en tidsperiod när uppgifterna får inplaceras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall skall upphovsmannen se över handlingarna minst vart femte år för att säkerställa att den ursprungliga säkerhetsklassningen fortfarande är nödvändig [Avsnitt III.10].	SECRET UE skall användas för på handlingar med beteckningen SECRET UE och, om detta är tillämpligt, förses med ESDP/PESD-märkning på mekanisk väg eller för hand [Avsnitt II.8]. EU-sekretessgrad skall anges centrerat i marginalen upptill och nedtill på varje sida, och varje sida skall numreras. På varje handling skall ett referensnummer och ett datum anges. Referensnumret skall anges på varje sida. Om flera kopior skall lämnas ut skall ett kopienummer anges på första sidan på varje exemplar, tillsammans med en uppgift om det totala antalet sidor. På första sidan skall det finnas en förteckning över alla bilagor och bifogade handlingar [Avsnitt VII.1].	Beslut om hävande av sekretessen eller inplacering i en lägre sekretessgrad får endast fattas av upphovsmannen, eller generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren som skall informera eventuella efterföljande mottagare till vilka de har lämnat ut eller kopierat handlingen om förändringen [Avsnitt III.9]. Handlingar med beteckningen SECRET UE skall förstöras av det register som är ansvarigt för dem under överinseende av en person som har genomgått säkerhetsprövning. Handlingar med beteckningen SECRET UE som förstörs skall förtecknas på undertecknade intyg om förstöring och bevaras av registret tillsammans med formulären om förstöring i minst tre år [Avsnitt VII.32].	Överskottskopior och handlingar som inte längre behövs måste förstöras [Avsnitt VII.31]. Handlingar med beteckningen SECRET UE, inklusive allt sekretessbelagt material som skall förstöras och som är resultatet av upprättande av handlingar med beteckningen SECRET UE, till exempel dåliga kopior, arbetsutkast, maskinskrivna noter och karbonpapper, skall förstöras genom att brännas, omvandlas till pappersmassa, gå genom en dokument förstörare eller på annat sätt reduceras så att de är oigenkännliga och icke möjliga att återställa [Avsnitt VII.31c och 32].

Säkerhetsklassning	När	Vem	Markeringar	Inplacering i en lägre sekretessgrad/hävande av sekretessen/förstöring	
				Vem	När
CONFIDENTIEL UE (hemligt): denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vålla Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen skada (ringa men). [Avsnitt II.3).	Att röja uppgifter med beteckningen CONFIDENTIEL UE kan: — påtagligt skada diplomatiska förbindelser, det vill säga förorsaka formella protester eller andra sanktioner, — äventyra enskilda personers säkerhet och frihet, — vålla skada på den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters styrkor, eller på effektiviteten hos värdefulla säkerhets- eller underrättelseoperationer, — väsentligt undergräva större organisationers finansiella livskraft, — hindra utredning av allvarliga brott eller göra det lättare att begå sådana, — väsentligt motarbeta EU:s eller medlemsstaternas finansiella, monetära, ekonomiska och kommersiella intressen, — allvarligt hindra utvecklingen eller genomförandet av EU:s viktigare strategier, — innebära ett avbrott för eller på annat sätt väsentligt störa betydelsefull EU-verksamhet	Medlemsstaterna: Befullmäktigade personer (upphovsmannen) [Avsnitt III.2]. Generalsekretariatet och EU:s decentraliserade organ: Behöriga personer (upphovsmannen) [Avsnitt III.2], generaldirektörer, generalsekreteraren/den höge representanten och ställföreträdande generalsekreteraren. Upphovsmannen skall ange ett datum eller en tidsperiod när uppgifterna får inplaceras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall skall upphovsmannen se över handlingarna minst vart femte år för att säkerställa att den ursprungliga säkerhetsklassningen fortfarande är nödvändig [Avsnitt III.10].	CONFIDENTIEL UE skall användas för på handlingar med beteckningen CONFIDENTIEL UE och, om detta är tillämpligt, förses med ESDP/PESD-märkning på mekanisk väg eller för hand [Avsnitt II.8]. EU:s sekretessgrad skall anges centrerat i marginalen upptill och nedtill på varje sida, och varje sida skall numreras. På första sidan skall det finnas en förteckning över alla bilagor och bifogade handlingar [Avsnitt VII.1].	Beslut om hävande av sekretessen eller inplacering i lägre sekretessgrad får endast fattas av upphovsmannen, eller generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren som skall informera eventuella efterföljande mottagare till vilka de har lämnat ut eller kopierat handlingen om förändringen [Avsnitt III.9]. Handlingar med beteckningen CONFIDENTIEL UE skall förstöras av det register som är ansvarigt för dessa handlingar under överinseende av en person som har genomgått säkerhetsprövning. Förstöringen av handlingarna skall registreras i enlighet med nationella bestämmelser och, när det gäller generalsekretariatet eller EU:s decentraliserade myndigheter, enligt instruktioner från generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren [Avsnitt VII.33].	Överskottskopior och handlingar som inte längre behövs måste förstöras [Avsnitt VII.31]. Handlingar med beteckningen CONFIDENTIEL UE, inklusive allt sekretessbelagt material som skall förstöras och som är resultatet av upprättande av handlingar med beteckningen CONFIDENTIEL UE, till exempel dåliga kopior, arbetsutkast, maskinskrivna noter och karbonpapper, skall förstöras genom att brännas, omvandlas till pappersmassa, gå genom en dokumentförstörare eller på annat sätt reduceras så att de är oigenkännliga och icke möjliga att återställa [Avsnitt VII.31c och 33].

Säkerhetsklassning	När	Vem	Markeringar	Inplacering i en lägre sekretessgrad/hävande av sekretessen/förstöring	
				Vem	När
RESTREINT UE (hemligt): denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vara till nackdel för Europeiska unionens eller en eller flera av dess medlemsstaters intressen. [Avsnitt II.4).	Att röja uppgifter med beteckningen RESTREINT UE kan: — påverka diplomatiska förbindelser på ett negativt sätt, — vålla väsentligt obehag för enskilda personer, — göra det svårare att upprätthålla den operativa effektiviteten eller säkerheten hos medlemsstaternas eller andra medverkande staters styrkor, — vålla finansiell förlust eller underlätta otillbörlig vinning eller fördel för enskilda personer eller företag, — medföra ett avbrott i korrekta åtaganden att upprätthålla förtroendet för uppgifter som tillhandahålls av tredje part, — medföra ett avbrott i lagstadgade restriktioner om yppande av uppgifter, — skada brottsutredningar eller göra det lättare att begå brott, — missgynna EU eller medlemsstaterna vid kommersiella eller strategiska förhandlingar med andra, — hindra en effektiv utveckling eller ett effektivt genomförande av EU:s strategier, — undergräva en god förvaltning av EU och dess operationer.	Medlemsstaterna: Behöriga personer (upphovsmannen) [Avsnitt III.2]. Generalsekretariatet och EU:s decentraliserade organ: Behöriga personer (upphovsmannen) [Avsnitt III.2], generalsekreteraren/den höge representanten och ställföreträdande generalsekreteraren. Upphovsmannen skall ange ett datum eller en tidsperiod när uppgifterna får inplaceras i en lägre sekretessgrad eller sekretessen kan hävas. I annat fall skall upphovsmannen se över handlingarna minst vart femte år för att säkerställa att den ursprungliga säkerhetsklassningen fortfarande är nödvändig [Avsnitt III.10].	Sekretessgraden RESTREINT UE skall tillämpas på handlingar med beteckningen RESTREINT UE och, om detta är tillämpligt, förses med ESDP/PESD-märkning på mekanisk eller elektronisk väg [Avsnitt II.8]. EU:s sekretessgrad skall anges centrerat i marginalen upptill och nedtill på varje sida, och varje sida skall numreras. På varje handling skall ett referensnummer och ett datum anges [Avsnitt VII.1].	Beslut om hävande av sekretessen eller inplacering i lägre sekretessgrad får endast fattas av upphovsmannen, eller generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren som skall informera eventuella efterföljande mottagare till vilka de har lämnat ut eller kopierat handlingen om förändringen [Avsnitt III.9]. Handlingar med beteckningen RESTREINT UE skall förstöras av det register som är ansvarigt för dessa handlingar i enlighet med nationella bestämmelser och, när det gäller generalsekretariatet eller EU:s decentraliserade myndigheter, enligt instruktioner från generalsekreteraren/den höge representanten eller ställföreträdande generalsekreteraren [Avsnitt VII.34].	Överskottskopior och handlingar som inte längre behövs måste förstöras [Avsnitt VII.31].

Tillägg 4

Riktlinjer för utlämnande av sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer

Samarbete på nivå 1

FÖRFARANDEN

1. Det är rådet som har behörighet att lämna ut sekretessbelagda EU-uppgifter till länder som inte har undertecknat Fördraget om Europeiska unionen eller andra internationella organisationer vilkas säkerhetspolitik och säkerhetsbestämmelser är jämförbara med EU:s.

2. Rådet får delegera beslutet att lämna ut sekretessbelagda uppgifter. I delegeringsbeslutet skall anges vilken typ av uppgifter som får lämnas ut och deras sekretessgrad, vilken normalt inte skall vara högre än CONFIDENTIEL UE.

3. Om ett säkerhetsavtal har ingåtts skall framställningar om att lämna ut sekretessbelagda EU-uppgifter lämnas in till generalsekreteraren/den höge representanten av de berörda staternas eller internationella organisationernas säkerhetsorgan som skall uppge för vilka ändamål utlämnandet är avsett och vilken typ av sekretessbelagda uppgifter som skall lämnas ut.

   Framställningar får också lämnas in av en medlemsstat eller en decentraliserad EU-myndighet som anser det önskvärt att sekretessbelagda EU-uppgifter lämnas ut. De skall uppge syftena och fördelen för EU med ett sådant utlämnande och specificera vilken typ av uppgifter som skall lämnas ut samt deras sekretessgrad.

4. Framställningen skall behandlas av generalsekretariatet som

   — skall begära yttranden av medlemsstaterna eller, om det är lämpligt, den decentraliserade EU-myndighet som är upphovsman till de uppgifter som skall lämnas ut,

   — skall upprätta de kontakter med mottagarländernas eller de internationella organisationernas säkerhetsorgan som är nödvändiga för att verifiera huruvida deras säkerhetspolitik eller säkerhetsbestämmelser är sådana att de utgör en garanti för att de sekretessbelagda uppgifterna som lämnas ut kommer att skyddas i enlighet med rådets säkerhetsbestämmelser,

   — skall begära tekniska yttranden av medlemsstaternas nationella säkerhetsmyndigheter beträffande den tilltro som kan sättas till mottagarstaterna eller de internationella organen.

5. Generalsekretariatet skall vidarebefordra framställningen och säkerhetsavdelningens rekommendation till rådet för beslut.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

6. Generalsekreteraren/den höge representanten skall informera mottagarstaterna eller de internationella organisationerna om rådets beslut om att ge tillstånd till att lämna ut sekretessbelagda EU-uppgifter och skicka så många exemplar av de här säkerhetsbestämmelserna som anses nödvändigt. Om framställningen har lämnats in av en medlemsstat skall denna stat informera mottagaren om att utlämnandet har godkänts.

   Beslutet om utlämnande skall inte träda i kraft förrän mottagarna ger en skriftlig försäkran om att de

   — inte kommer att använda uppgifterna för andra ändamål än de som har överenskommits,

   — kommer att skydda uppgifterna i enlighet med säkerhetsbestämmelserna och i synnerhet de särskilda bestämmelser som anges nedan.

7. *Personal*

   a) Antalet tjänstemän med tillgång till sekretessbelagda EU-uppgifter skall vara starkt begränsat och grundas på principen om att endast de personer som behöver uppgifterna för sin tjänsteutövning skall ha tillgång till dem.

b) Alla tjänstemän och medborgare som är behöriga att ha tillgång till uppgifter med beteckningen "CONFIDENTIEL UE" eller högre sekretessgrad skall inneha antingen ett säkerhetsintyg på tillämplig nivå eller ett motsvarande intyg på genomgången säkerhetsprövning, och detta intyg, oberoende av vilketdera, skall utfärdas av regeringen i deras egen stat.

8. *Vidarebefordran/överföring av handlingar*

a) De praktiska förfarandena för vidarebefordran/överföring av handlingar skall beslutas genom överenskommelse på grundval av bestämmelserna i avsnitt VII i rådets säkerhetsbestämmelser. I dessa förfaranden skall det i synnerhet specificeras till vilka register sekretessbelagda EU-uppgifter skall skickas.

b) Om de sekretessbelagda uppgifter vilkas utlämnande rådet ger tillstånd till inbegriper handlingar med beteckningen "TRÈS SECRET UE/EU TOP SECRET" skall mottagarstaten eller den internationella organisationen inrätta ett centralt register för EU och vid behov en underavdelning. Dessa register skall omfattas av bestämmelserna i avsnitt VIII i rådets säkerhetsbestämmelser.

9. *Registrering*

Så snart som ett register mottar en EU-handling med beteckningen "CONFIDENTIEL UE" eller högre sekretessgrad skall det diarieföra den inkomna handlingen i ett diarium som innehåller spalter för datum för mottagande, uppgifter om dokumentet (datum, referens- och kopienummer), dess säkerhetsklassning, titel, mottagarens namn eller titel, datum för återlämnande av kvitto och det datum då handlingen återsänds till upphovsmannen inom EU eller förstörs.

10. *Förstöring*

a) Sekretessbelagda EU-handlingar skall förstöras i enlighet med instruktionerna i avsnitt VI i rådets säkerhetsbestämmelser. Kopior av intygen om förstöring av för handlingar med sekretessgrad "SECRET UE och TRÈS SECRET UE/EU TOP SECRET" skall sändas till det register inom EU som översänt handlingarna.

b) Sekretessbelagda EU-handlingar skall omfattas av de beredskapsplaner för dokumentförstöring som de mottagande organen har för sina egna sekretessbelagda handlingar.

11. *Skydd av handlingar*

Alla åtgärder skall vidtas för att hindra obehöriga från att få tillgång till sekretessbelagd EU-information.

12. *Kopior, översättningar och utdrag*

Handlingar med sekretessgraderna "CONFIDENTIEL UE och SECRET UE" får inte kopieras eller översättas och inga utdrag för göras utan medgivande från chefen för den berörda säkerhetsorganisationen, som skall registrera och kontrollera dessa kopior, översättningar och utdrag samt, om så behövs, anbringa stämpel.

Kopiering eller översättning av en handling med sekretessgraden "TRÈS SECRET UE/EU TOP SECRET" får beviljas endast av den myndighet som upprättat handlingen, vilken skall ange hur många kopior som får göras. Om det inte kan fastställas vilken myndighet som upprättat handlingen skall begäran riktas till generalsekretariatets säkerhetsavdelning.

13. *Sekretessbrott*

Om sekretessbrott vad gäller sekretessbelagda EU-handlingar har skett eller misstänks skall följande åtgärder genast vidtas i enlighet med det ingångna säkerhetsavtalet:

a) En undersökning skall genomföras för att fastställa de omständigheter under vilka sekretessen brutits.

b) Generalsekretariatets säkerhetsavdelning, den nationella säkerhetsmyndigheten och den myndighet som upprättat handlingen skall underrättas, eller så skall det i förekommande fall klart anges att den sistnämnda inte har underrättats.

c) Åtgärder skall vidtas för att minimera verkningarna av sekretessbrottet.

d) Åtgärderna skall ses över och åtgärder skall vidtas för att förhindra att det inträffade upprepas.

e) Alla åtgärder som anbefalls av rådets säkerhetsavdelning för att förhindra att det inträffade upprepas skall genomföras.

14. *Inspektioner*

Rådets säkerhetsavdelning skall genom avtal med berörda stater eller internationella organisationer ha behörighet att göra en bedömning av åtgärdernas effektivitet för att skydda de sekretessbelagda EU-uppgifter som lämnats ut.

15. *Rapportering*

I enlighet med ingånget säkerhetsavtal skall den stat eller internationella organisation som fått tillgång till sekretessbelagda EU-uppgifter årligen vid en tidpunkt som fastställdes när tillståndet att lämna ut informationen gavs överlämna en rapport i vilken det bekräftas att de här säkerhetsbestämmelserna efterlevts.

Tillägg 5

Riktlinjer för utlämnande av sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer

Samarbete på nivå 2

RUTINER

1. Rätten att lämna ut sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer, vilkas säkerhetspolitik och säkerhetsbestämmelser markant skiljer sig från vad som tillämpas av EU, tillkommer rådet. I princip är rätten begränsad till information med sekretessgrad upp till och med SECRET UE; den omfattar inte nationell information som är särskilt förbehållen medlemsstaterna och sådana sekretessbelagda EU-uppgifter som skyddas genom särskild märkning.

2. Rådet får delegera beslutet. När ett beslut delegeras inom de begränsningar som anges i punkt 1 skall rådet ange vilket slag av information som får lämnas ut och sekretessgraden på denna, som inte får vara högre än RESTREINT UE.

3. I enlighet med ingånget säkerhetsavtal skall framställningar om att lämna ut sekretessbelagda EU-uppgifter göras till generalsekreteraren/den höge representanten av den berörda statens eller internationella organisationens säkerhetsorgan, som skall ange för vilka syften uppgifterna är ämnade samt arten av och sekretessgraden på det som eventuellt lämnas ut.

   Framställningar får också göras av en medlemsstat eller en decentraliserad EU-myndighet som betraktar utlämnandet av sekretessbelagd information som önskvärt. De skall då ange syftet med och nyttan för EU av att informationen lämnas ut samt ange arten av och sekretessgraden på det som kan komma att lämnas ut.

4. Framställningen skall behandlas av generalsekretariat, som skall

   — begära in yttrande från den medlemsstat eller, i förekommande fall, den decentraliserade EU-myndighet som är upphovsman till de uppgifter som eventuellt skall lämnas ut,

   — ta inledande kontakter med den mottagande statens eller internationella organisationens säkerhetsorgan för att få information om deras säkerhetspolitik och deras säkerhetsbestämmelser samt upprätta en jämförande tablå över de säkerhetsklasser som tillämpas inom EU och den berörda staten eller organisationen,

   — anordna ett möte i rådets säkerhetskommitté eller, vid behov med förenklat skriftligt förfarande, begära att medlemsstaternas nationella säkerhetsmyndigheter skall utverka säkerhetskommitténs tekniska utlåtande.

5. Det tekniska utlåtandet från rådets säkerhetskommitté skall ta upp följande punkter:

   — Vilket förtroende man kan hysa för den mottagande staten eller internationella organisationen med tanke på bedömningen av säkerhetsriskerna för EU eller dess medlemsstater.

   — En bedömning av mottagarens förmåga att skydda de sekretessbelagda uppgifter som EU lämnar ut.

   — Förslag till praktiska rutiner för hantering av sekretessbelagda EU-uppgifter (exempelvis att man överlämnar "tvättade" versioner av en text) och EU-handlingar som vidarebefordras/överförs (genom att man bibehåller alternativt stryker rubricering av EU:s säkerhetsklassning, särskilda markeringar m.m.).

   — Inplacering i lägre sekretessgrad eller hävande av sekretessen genom den myndighet som är upphovsman innan uppgifterna lämnas ut till de mottagande länderna eller internationella organisationerna. ([1]).

([1]) Detta innebär att den myndighet som är upphovsman till uppgifterna i fråga om samtliga kopior som lämnats ut inom EU skall tillämpa det förfarande som anges i avsnitt III punkt 9.

6. Generalsekreteraren/den höge representanten skall överlämna framställningen och det tekniska utlåtande från rådets säkerhetskommitté som rådets säkerhetsavdelning erhållit till rådet för beslut.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

7. Rådets beslut om att tillåta utlämnande av sekretessbelagd EU-information skall av generalsekreteraren/den höge representanten tillsammans med en jämförande tablå över de säkerhetsklasser som tillämpas inom EU och de berörda staterna eller organisationerna tillställas de mottagande länderna eller internationella organisationerna. Om det är en medlemsstat som gjort framställningen skall denna stat underrätta mottagaren om att utlämnandet har beviljats.

Beslutet om att lämna ut uppgifter skall träda i kraft endast om mottagarna lämnar skriftlig försäkran om att de

— inte kommer att använda informationen för några andra syften än de man kommit överens om,

— kommer att skydda uppgifterna i enlighet med de bestämmelser som rådet fastställt.

8. Följande skyddsföreskrifter skall upprättas såvida inte rådet efter det att det mottagit det tekniska utlåtandet från rådets säkerhetskommitté beslutar om ett särskilt förfarande för handhavandet av sekretessbelagda EU-handlingar (genom att man avlägsnar uppgifter om EU:s sekretessgrad, särskilda markeringar m.m.).

Dessa föreskrifter skall i så fall antas.

9. *Personal*

a) Det antal tjänstemän som ges tillgång till sekretessbelagda EU-uppgifter måste hållas strikt begränsat till att endast omfatta sådana personer vars åligganden kräver sådan tillgång och bygga på principen om vad personen behöver veta för sin tjänsteutövning.

b) Samtliga tjänstemän och egna medborgare som ges tillgång till den sekretessbelagda information som lämnas ut av EU skall ha genomgått säkerhetsprövning eller ha rätt till tillgång till nationell sekretessbelagd information på erforderlig nivå motsvarande EU:s nivå enligt den jämförande tablån.

c) De nationella säkerhetsprövningen eller tillståndsgivningen skall för kännedom tillställas generalsekreteraren/den höge representanten.

10. *Vidarebefordran av handlingar*

a) De praktiska rutinerna för att vidarebefordra handlingar skall beslutas gemensamt av generalsekretariatets säkerhetsavdelning och de mottagande staternas eller internationella organisationernas säkerhetsorgan på grundval av de regler för detta som anges i avsnitt VII i dessa bestämmelser. Därvid skall bland annat anges de exakta adresser till vilka handlingarna skall sändas samt vilket bud- eller kurirföretag som anlitas för att befordra den sekretessbelagda EU-informationen.

b) Handlingar med sekretessgraden CONFIDENTIEL UE och högre skall placeras i dubbla kuvert. Innerkuvertet skall markeras ”EU” och sekretessgraden skall anges på det kuvertet. Ett mottagningsbevis för varje sekretessbelagd handling skall medsändas. På mottagningsbeviset, vilket inte är sekretessbelagt, skall endast vissa särskilda uppgifter rörande handlingen anges (dess referensnummer, datum, kopians nummer) liksom det språk på vilken den är avfattad, men däremot inte titeln på handlingen.

c) Innerkuvertet skall därpå placeras i ytterkuvertet, vilket måste ha ett försändelsenummer för att möjliggöra förfarandet med mottagningsbevis. På ytterkuvertet skall ingen sekretessgrad anges.

d) Ett mottagningsbevis av vilket försändelsens nummer framgår skall alltid lämnas till budet.

11. *Diarieföring vid ankomsten*

Den mottagande statens nationella säkerhetsmyndighet eller det motsvarande organ i den staten som på sin regerings vägnar tar emot sekretessbelagd information som vidarebefordrats av EU, eller säkerhetsavdelningen på den mottagande internationella organisationen, skall upprätta ett särskilt register för att diarieföra sekretessbelagd information från EU efter hand som denna mottas. Registret skall ha kolumner för mottagningsdatum, särskilda uppgifter rörande handlingen (datum, referensnummer och antalet exemplar), sekretessgrad, titel, mottagarens namn eller titel, datum för mottagningsbevisets returnering samt datum för handlingens returnering till EU alternativt för dess förstörande.

12. *Returnering av handlingar*

När mottagaren returnerar en sekretessbelagd handling till rådet eller till den medlemsstat som lämnat ut denna skall denne förfara i enlighet med punkt 10.

13. *Skydd*

a) När handlingarna inte används skall de arkiveras i ett säkerhetsskåp som godkänts för arkivering av nationellt sekretessbelagt material med samma sekretessgrad. Detta förvaringsskåp får inte vara försett med någon uppgift om innehållet, vilket endast skall vara åtkomligt för personer som bemyndigats att hantera sekretessbelagd EU-information. Om kombinationslås används får kombinationen endast vara känd av de tjänstemän inom staten eller organisationen som har rätt att ha tillgång till den sekretessbelagda EU-information som förvaras i förvaringsskåpet och kombinationen måste bytas ut var sjätte månad, eller tidigare, om en tjänsteman förflyttas, om resultatet av säkerhetsprövningen av någon av de tjänstemän som känner till kombinationen återkallas eller om det föreligger risk för sekretessbrott.

b) Sekretessbelagda EU-handlingar får avlägsnas ur säkerhetsskåpet endast av tjänstemän som genomgått säkerhetsprövning för tillgång till sekretessbelagd EU-information och som för sin tjänsteutövning behöver känna till deras innehåll. De skall vara ansvariga för att handlingarna förvaras på betryggande sätt så länge som de hanterar dem och framför allt se till att ingen obehörig får tillgång till handlingarna. De skall också se till att handlingarna åter arkiveras i säkerhetsskåpet när de tagit del av dem samt utanför arbetstid.

c) Inga kopior av eller utdrag ur får göras av handlingar med sekretessgraden CONFIDENTIEL UE eller högre utan att rådets säkerhetsavdelning lämnat sitt medgivande.

d) Det skall tillsammans med rådets säkerhetsavdelning fastställas och bekräftas hur handlingarna i en nödsituation snabbt och fullständigt kan förstöras.

14. *Fysisk säkerhet*

a) Säkerhetsskåp som används för arkivering av sekretessbelagd EU-information skall permanent hållas låsta.

b) Om underhålls- eller städpersonal behöver gå in i eller arbeta i en lokal där sådana säkerhetsskåp finns, skall de hela tiden åtföljas av en medarbetare ur statens eller organisationens säkerhetstjänst eller av en tjänsteman med specifikt ansvar för lokalens övervakning.

c) Utanför ordinarie arbetstid (nattetid, under veckoslut och allmänna helgdagar) skall de säkerhetsskåp där sekretessbelagd EU-information förvaras skyddas av antingen vakt eller automatisk larmanordning.

15. *Sekretessbrott*

Om ett sekretessbrott har förekommit eller misstänks ha förekommit i fråga om sekretessbelagda EU-handlingar skall följande åtgärder genast vidtas:

a) En rapport skall omgående tillställas rådets säkerhetsavdelning eller den nationella säkerhetsmyndigheten i den medlemsstat som tagit initiativet till att vidarebefordra handlingarna (med kopia till rådets säkerhetsavdelning).

b) En utredning skall genomföras, varefter en uttömmande rapport skall lämnas säkerhetsorganet (se föregående punkt a). Nödvändiga ändringar för att åtgärda bristerna skall därefter genomföras.

16. *Inspektioner*

Rådets säkerhetsavdelning skall genom överenskommelse med de berörda staterna eller internationella organisationerna ha rätt att utvärdera åtgärderna för att skydda de sekretessbelagda EU-uppgifter som lämnats ut.

17. *Rapportering*

Så länge en stat eller organisation i sitt förvar har sekretessbelagd EU-information skall den årligen vid en tidpunkt som fastställdes när tillståndet att lämna ut informationen gavs lägga fram en rapport i vilken det bekräftas att de här säkerhetsbestämmelserna har efterlevts.

Tillägg 6

Riktlinjer för utlämnande av sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer

Samarbete på nivå 3

RUTINER

1. Rådet kan under vissa särskilda förhållanden önska samarbeta med stater eller organisationer som inte kan lämna den försäkran som krävs i de här säkerhetsbestämmelserna samtidigt som samarbetet kan påkalla att sekretessbelagda EU-uppgifter lämnas ut. Sådan utlämning får inte omfatta nationell information som är särskilt förbehållen medlemsstaterna.

2. Under sådana särskilda förhållanden skall framställningar om samarbete med EU, oavsett om de kommer från tredje land eller från internationella organisationer och om de föreslås av medlemsstaterna eller eventuellt av decentraliserade EU-myndigheter, först i sak behandlas av rådet, som vid behov skall begära in yttrande från den medlemsstat eller decentraliserade myndighet som är upphovsman till uppgifterna. Rådet skall överväga det välbetänkta i att lämna ut sekretessbelagd information, bedöma mottagarnas behov av att för tjänsteändamål få tillgång till denna samt besluta om vilket slag av sekretessbelagd information som får överlämnas.

3. Om rådet tillstyrker skall det åvila generalsekreteraren/den höge representanten att sammankalla rådets säkerhetskommitté eller begära att medlemsstaternas nationella säkerhetsmyndigheter, vid behov med förenklat skriftligt förfarande, skall utverka säkerhetskommitténs tekniska utlåtande.

4. Utlåtandet från rådets säkerhetskommitté skall ta upp följande punkter:

   a) En bedömning av vilka säkerhetsrisker som EU eller dess medlemsstater löper.

   b) Sekretessgraden på den information som får lämnas ut, där så behövs med hänsyn till informationens art.

   c) Inplacering i lägre sekretessgrad eller hävande av sekretessen genom den myndighet som är upphovsman till uppgifterna innan den lämnas ut till de berörda länderna eller internationella organisationerna ([1]).

   d) Rutiner för hanteringen av de handlingar som skall lämnas ut (se punkt 5 nedan).

   e) De sätt på vilka vidarebefordran/överföringen får ske (användning av offentliga posttjänster, allmänna eller säkra system för telekommunikation, diplomatisk kurirförsändelse, bud som genomgått säkerhetsprövning m.m.).

5. De handlingar som lämnas ut till stater och organisationer som omfattas av denna bilaga skall i princip färdigställas utan omnämnande av källan eller EU:s sekretessgrad. Rådets säkerhetskommitté kan anbefalla

   — användning av särskild markering eller kodbeteckning,

   — användning av ett särskilt säkerhetsklassningssystem, varigenom informationens känslighet kopplas till de kontrollåtgärder som erfordras på grund av det sätt som valts för vidarebefordran/översändning av handlingarna (se exempel i punkt 14).

6. Rådets säkerhetsavdelning skall överlämna säkerhetskommitténs tekniska utlåtande till rådet, om så behövs tillsammans med den delegering av befogenheter som krävs för uppgiftens utförande, något som särskilt är aktuellt i akuta lägen.

7. Efter det att rådet godkänt att sekretessbelagda EU-uppgifter lämnas ut och hur detta praktiskt skall genomföras, skall rådets säkerhetsavdelning med den berörda statens eller organisationens säkerhetsorgan upprätta den nödvändiga kontakten för att befrämja att de avsedda säkerhetsåtgärderna tillämpas.

([1]) Detta innebär att den myndighet som är upphovsman till uppgifterna i fråga om samtliga kopior som lämnats ut inom EU skall tillämpa det förfarande som anges i avsnitt III punkt 9.

8. Som referens skall i enlighet med rådets beslut rådets säkerhetsavdelning tillställa samtliga medlemsstater, samt vid behov berörda decentraliserade EU-myndigheter, en uppställning i vilken informationens art och säkerhetsklassning sammanfattas och där de organisationer och länder anges till vilka den får utlämnas.

9. Den nationella säkerhetsmyndigheten i den medlemsstat som lämnar ut handlingar, eller rådets säkerhetsavdelning, skall vidta alla de åtgärder som behövs för att underlätta framtida skadebedömningar och översyn av rutinerna.

10. Ärendet skall även i fortsättningen hänskjutas till rådet närhelst förutsättningarna för samarbetet ändras.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

11. Rådets beslut om att tillåta utlämnande av sekretessbelagda EU-uppgifterna skall av generalsekreteraren/den höge representanten tillställas de mottagande staterna eller internationella organisationerna tillsammans med de skyddsföreskrifter som föreslagits av rådets säkerhetskommitté och godkänts av rådet. Om det är en medlemsstat som gjort framställningen skall denna stat underrätta mottagaren om att utlämnandet har beviljats.

Beslutet skall verkställas endast om mottagarna lämnar skriftlig försäkran om att de

— inte kommer att använda informationen för några andra syften än det samarbete som rådet beslutat om,

— kommer att skydda uppgifterna på det sätt som rådet kräver.

12. *Vidarebefordran av handlingar*

a) De praktiska rutinerna för att vidarebefordra handlingar skall beslutas gemensamt av generalsekretariatets säkerhetsavdelning och de mottagande staternas eller internationella organisationernas säkerhetsorgan. Det skall därvid bland annat anges de exakta adresser till vilka handlingarna skall vidarebefordras.

b) Handlingar med sekretessgraden ”CONFIDENTIEL UE” och högre skall placeras i dubbla kuvert. Innerkuvertet skall förses med den särskilda stämpel eller kodbeteckning man beslutat om och det skall på detta kuvert anges den särskilda säkerhetsklassning som godkänts för dokumentet. Ett mottagningsbevis för varje sekretessbelagd handling skall medsändas. På mottagningsbeviset, vilket inte är sekretessbelagt, skall endast vissa särskilda uppgifter rörande handlingen anges (dess referensnummer, datum, kopians nummer) liksom det språk på vilken den är avfattad, men däremot inte titeln på handlingen.

c) Innerkuvertet skall därpå placeras i ytterkuvertet, vilket måste ha ett försändelsenummer för att möjliggöra förfarandet med mottagningsbevis. På ytterkuvertet skall ingen sekretessgrad anges.

d) Ett mottagningsbevis av vilket försändelsens nummer framgår skall alltid lämnas till budet.

13. *Diarieföring vid ankomsten*

Den mottagande statens nationella säkerhetsmyndighet eller det motsvarande organ i den staten som på sin regerings vägnar tar emot sekretessbelagd information som vidarebefordrats av EU, eller säkerhetsavdelningen vid den mottagande internationella organisationen, skall upprätta ett särskilt register för att diarieföra sekretessbelagd information från EU efter hand som denna mottas. Registret skall ha kolumner för mottagningsdatum, särskilda uppgifter rörande handlingen (datum, referensnummer och antalet exemplar), sekretessgrad, titel, mottagarens namn eller titel, datum för mottagningsbevisets returnering samt datum för handlingens returnering till EU alternativt för dess förstörande.

14. *Användning och skydd av sekretessbelagda uppgifter som lämnats ut*

a) Uppgifter med sekretessgraden ”SECRET UE” skall hanteras av särskilt utsedda tjänstemän som bemyndigats att ha tillgång till information med denna sekretessgrad. Den skall arkiveras i väl inrättade säkra förvaringsrum, som endast kan öppnas av personer som bemyndigats att ha tillgång till den information som finns där. De utrymmen där dessa rum är belägna skall stå under permanent bevakning och ett kontrollförfarande skall inrättas för att säkerställa att endast vederbörligen bemyndigade personer beviljas tillträde. Uppgifter med sekretessgraden ”SECRET UE” skall översändas med diplomatisk kurirförsändelse, säkra postföretag och säkra telekommunikationsmedel. En handling med sekretessgraden ”SECRET UE” får mångfaldigas endast efter skriftligt medgivande från den myndighet som är upphovsman. Samtliga exemplar skall registreras och följas upp. Mottagningsbevis skall utfärdas för alla åtgärder som berör handlingar med sekretessgraden ”SECRET UE”.

b) Uppgifter med sekretessgraden "CONFIDENTIEL UE" skall hanteras av i vederbörlig ordning utsedda tjänstemän som har behörighet att få information om ärendet. Handlingarna skall arkiveras i säkra låsta förvaringsrum i övervakade utrymmen.

Uppgifter med sekretessgraden "CONFIDENTIEL UE" skall översändas med diplomatisk kurirförsändelse, militär postgång och säkra telekommunikationsmedel. Det mottagande organet får göra kopior, vilkas antal och utlämning skall noteras i särskilda register.

c) Uppgifter med sekretessgraden "RESTREINT UE" skall hanteras i lokaler till vilka obehöriga personer inte har tillträde och arkiveras i låsta skåp. Handlingar får som rekommenderade försändelser sändas med allmän postbefordran i dubbla kuvert och, i nödfall under en pågående verksamhet, med icke skyddade allmänna telekommunikationssystem. Mottagarna får göra kopior.

d) Icke sekretessbelagda uppgifter bör inte påkalla särskilda skyddsåtgärder och får sändas med post och offentliga telekommunikationsmedel. Mottagarna får göra kopior.

15. *Förstöring*

Handlingar som inte längre behövs skall förstöras. I fråga om sekretessgraderna "RESTREINT UE" och "CONFIDENTIEL UE" skall detta noteras i de särskilda registren. I fråga om handlingar med sekretessgraden SECRET UE skall ett intyg utfärdas och undertecknas av två personer som bevittnat förstöringen av handlingen.

16. *Sekretessbrott*

Om uppgifter med sekretessgraden "CONFIDENTIEL UE" eller "SECRET UE" kommit ut eller om det finns misstanke om att så skett skall den nationella säkerhetsmyndigheten i den berörda staten eller säkerhetschefen i den berörda organisationen utreda omständigheterna kring det inträffade. Om utredningen bekräftar misstankarna skall den myndighet som är upphovsman underrättas. Nödvändiga åtgärder skall vidtas för att rätta till bristande rutiner eller arkiveringsmetoder om dessa legat till grund för läckan. Rådets generalsekreterare/höge företrädare eller den nationella säkerhetsmyndigheten i den medlemsstat som lämnat ut de uppgifterna som röjts bör av mottagaren begära en detaljerad redogörelse rörande utredningen.