II

(Rättsakter vilkas publicering inte är obligatorisk)

KOMMISSIONEN

KOMMISSIONENS BESLUT
av den 29 november 2001
om ändring av de interna stadgarna

[delgivet med nr K(2001) 3031]

(2001/844/EG, EKSG, Euratom)

EUROPEISKA GEMENSKAPERNAS KOMMISSION HAR FATTAT DETTA BESLUT

med beaktande av Fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 218.2 i detta,

med beaktande av Fördraget om upprättandet av Europeiska kol- och stålgemenskapen, särskilt artikel 16 i detta,

med beaktande av Fördraget om upprättandet av Europeiska atomenergigemenskapen, särskilt artikel 131 i detta,

med beaktande av Fördraget om upprättandet av Europeiska unionen, särskilt artikel 28.1 och artikel 41.1 i detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Kommissionens säkerhetsbestämmelser, som finns som bilaga till detta beslut, fogas härmed till kommissionens interna stadgar som bilaga.

Artikel 2

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

Det skall tillämpas från den 1 december 2001.

Utfärdat i Bryssel den 29 november 2001.

På kommissionens vägnar

Romano PRODI

Ordförande

BILAGA

KOMMISSIONENS SÄKERHETSBESTÄMMELSER

av följande skäl:

(1) För att kommissionens verksamhet skall kunna utvecklas på sådana områden som kräver en hög grad av sekretess bör ett övergripande säkerhetssystem upprättas som omfattar kommissionen, andra institutioner, organ och kontor som upprättats genom eller på grundval av EG-fördraget eller Fördraget om Europeiska unionen, medlemsstaterna samt andra mottagare av sekretessbelagda uppgifter från EU, nedan kallat sekretessbelagda EU-uppgifter.

(2) För att garantera att det säkerhetssystem som upprättas genom denna förordning är effektivt kommer kommissionen endast tillhandahålla sekretessbelagda EU-uppgifter till de utomstående organ som kan ge garantier för att de har vidtagit alla åtgärder som krävs för att följa dessa bestämmelser.

(3) Dessa bestämmelser antas utan att det påverkar förordning nummer 3 av den 31 juli 1958 om genomförandet av artikel 24 i Fördraget om upprättandet av Europeiska atomenergigemenskapen [1], rådets förordning 1588/90 av den 11 juni 1990 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor [2] och utan att det påverkar kommissionens beslut C (95) 1510 slutlig av den 23 november 1995 on the protection of informatics systems (ej översatt till svenska).

(4) Kommissionens säkerhetssystem bygger på principerna i rådets beslut 2001/264/EG av den 19 mars 2001 om antagande av rådets säkerhetsbestämmelser [3] för att unionens beslutsprocess skall kunna fungera på ett smidigt sätt.

(5) Kommissionen betonar vikten av att i förekommande fall låta övriga institutioner omfattas av de regler och normer för sekretess som är nödvändiga för att skydda unionens och medlemsstaternas intressen.

(6) Kommissionen behöver egna principer för sekretess med beaktande av alla säkerhetsaspekter samt kommissionens särskilda ställning som institution.

(7) Dessa bestämmelser antas utan att det påverkar artikel 255 i fördraget eller Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar [4].

Artikel 1

Kommissionens säkerhetsbestämmelser fastställs i bilagan.

Artikel 2

1. När det gäller hantering av sekretessbelagda EU-uppgifter skall den ledamot av kommissionen som ansvarar för säkerhetsfrågor vidta lämpliga åtgärder för att se till att de bestämmelser som avses i artikel 1 iakttas inom kommissionen av kommissionens tjänstemän och andra anställda, av avdelad personal från kommissionen samt i alla kommissionens byggnader, inbegripet representationer och kontor i unionen och på delegationer i tredjeländer samt av uppdragstagare utanför kommissionen.

2. Medlemsstaterna, andra institutioner, organ och kontor som upprättats genom eller på grundval av fördragen skall ha tillåtelse att motta sekretessbelagda EU-uppgifter under förutsättning att de, då sekretessbelagda EU-uppgifter hanteras, ser till att bestämmelserna i punkt 1 följs på deras enheter och i deras lokaler, särskilt av följande kategorier:

a) Anställda vid medlemsstaternas ständiga representationer vid Europeiska unionen och av de nationella delegationer som deltar i kommissionsmöten eller i möten i kommissionens organ, eller som deltar i annan verksamhet som leds av kommissionen.

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

c) Utomstående uppdragstagare och avdelad personal som hanterar sekretessbelagda EU-uppgifter.

[1] EGT 17/58, 6.10.1958, s. 406/58.
[2] EGT L 151, 15.6.1990, s. 1.
[3] EGT L 101, 11.4.2001, s. 1.
[4] EGT L 145, 31.5.2001, s. 43.

Artikel 3

Tredjeländer, internationella organisationer och andra organ skall tillåtas att motta sekretessbelagda EU-uppgifter under förutsättning att de, då dessa uppgifter hanteras, strikt följer bestämmelserna i artikel 1.

Artikel 4

I överensstämmelse med de grundläggande principer och miniminormer för säkerhet som återfinns i del I av bilagan, får den ledamot av kommissionen som ansvarar för säkerhetsfrågor vidta åtgärder i enlighet med del II i bilagan.

Artikel 5

Föreliggande bestämmelser skall från dagen för antagandet ersätta

a) Kommissionens beslut C (94) 3282 av den 30 november 1994 on the security measures applicable to classified information produced or transmitted in connection with activities of the European Union (ej översatt till sv).

b) Kommissionens beslut C (1999) 423 av den 25 februari 1999 relating to the procedures whereby officials and other employees of the European Commission may be allowed access to classified information held by the Commission (ej översatt till sv.).

Artikel 6

Från och med det att dessa bestämmelser träder i kraft skall följande gälla för alla sekretessbelagda uppgifter som till och med det datumet innehas av kommissionen, utom sekretessbelagda Euratom-uppgifter:

a) Om uppgifterna kommer från kommissionen skall de klassas på nytt som EU RESTRICTED, såvida inte upphovsmannen beslutar om annan klassning senast den 31 januari 2002. I så fall skall upphovsmannen underrätta alla mottagare av dokumentet i fråga.

b) Om uppgifterna kommer utifrån skall kommissionen behålla den ursprungliga klassificeringen och behandla uppgifterna som sekretessbelagda EU-uppgifter på motsvarande nivå, såvida inte upphovsmannen samtycker till hävande av sekretess eller inplacering i lägre sekretessgrad.

BILAGA

SÄKERHETSBESTÄMMELSER

Innehåll

-

DEL I: GRUNDLÄGGANDE PRINCIPER OCH MINIMINORMER FÖR SÄKERHET

1. INLEDNING

I dessa bestämmelser fastställs de grundläggande principer och miniminormer för säkerhet som skall följas på korrekt sätt av kommissionen på alla dess avdelningar, samt av alla mottagare av sekretessbelagda EU-uppgifter, så att säkerheten garanteras och var och en kan vara förvissad om att gemensamma skyddsnormer för säkerheten har fastställts.

2. ALLMÄNNA PRINCIPER

Kommissionens säkerhetspolitik är en integrerad del av dess allmänna interna förvaltningspolitik och grundar sig således på de principer som ligger till grund för dess allmänna politik.

Dessa principer innefattar lagenlighet, öppenhet och insyn, ansvarsskyldighet och subsidiaritet (proportionalitet).

Lagenlighet innebär behovet att strikt följa de rättsliga ramarna i genomförandet av säkerhetsföreskrifterna och behovet att följa de rättsliga kraven. Det innebär också att ansvaret på säkerhetsområdet skall grunda sig på vederbörliga rättsliga bestämmelser. Bestämmelserna i tjänsteföreskrifterna gäller till fullo, särskilt dess artikel 17 om personalens skyldighet att tillämpa diskretion när det gäller kommissionens uppgifter samt dess avdelning VI om disciplinära åtgärder. Slutligen innebär det att sekretessbrott inom kommissionens ansvarsområde måste hanteras på ett sätt som överensstämmer med kommissionens politik om disciplinära åtgärder samt dess politik om samarbete med medlemsstaterna på det kriminalrättsliga området.

Öppenhet och insyn innebär behovet av tydlighet avseende alla säkerhetsbestämmelser och föreskrifter, för balans mellan olika tjänster och olika områden (fysisk säkerhet gentemot informationsskydd osv.) samt behovet av en konsekvent och strukturerad säkerhetsmedveten politik. Det definierar också behovet av tydliga skriftliga riktlinjer för genomförande av säkerhetsåtgärder.

Ansvarsskyldighet innebär att ansvarsförhållanden på säkerhetsområdet kommer att klart definieras. Dessutom anger det behovet av att regelbundet kontrollera om dessa ansvarsplikter har fullgjorts korrekt.

Subsidiaritet eller proportionalitet innebär att säkerhet skall organiseras på lägsta möjliga nivå och så nära generaldirektoraten och kommissionen som möjligt. Det anger också att säkerhetsverksamheten skall begränsas till de delar där den verkligen behövs. Slutligen innebär det att säkerhetsåtgärderna skall stå i proportion till de intressen som skall skyddas och till det faktiska och potentiella hotet mot dessa intressen, för att möjliggöra ett skydd som orsakar minsta möjliga störning.

3. SÄKERHETSGRUNDERNA

Grunderna för god säkerhet är följande:

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

   (1) insamling och registrering av underrättelser om spionerі, sabotage, terrorism och annan omstörtande verksamhet, och

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

b) I varje medlemsstat och på kommissionen, 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 och berörda avdelningar inom de europeiska institutionerna, för att i tillämpliga fall fastställa och rekommendera

   (1) vilka personer, uppgifter och resurser som behöver skydd, och

   (2) gemensamma skyddsnormer.

d) Nära samarbete mellan kommissionens säkerhetsavdelning och säkerhetsavdelningarna på andra europeiska institutioner samt med NATO:s säkerhetsavdelning (NOS).

4. PRINCIPER FÖR INFORMATIONSSÄKERHET

4.1 **Mål**

Informationssäkerheten 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 sekretess, okränkbarhet och tillgänglighet,

c) att skydda kommissionens lokaler 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.

4.2 **Definitioner**

I dessa bestämmelser används följande begrepp:

a) Sekretessbelagda EU-uppgifter omfattar alla uppgifter och all materiel, som om de röjdes av obehöriga 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, tredjeland eller internationella organisationer.

b) Handling är varje 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.

c) Material är en handling enligt definitionen under punkt b samt varje slags utrustning som antingen har tillverkats eller håller på att tillverkas.

d) Behov av uppgifter innebär en enskild anställds behov av att få tillgång till sekretessbelagda EU-uppgifter för att kunna genomföra sitt arbete eller sin uppgift.

e) Tillstånd innebär att kommissionens ordförande beslutar att ge en enskild individ tillgång till sekretessbelagda EU-uppgifter i angiven omfattning, efter ett positivt resultat av en säkerhetsprövning (granskning) som genomförts av den nationella säkerhetsmyndigheten enligt nationell lag.

f) Klassificering innebär att uppgifter ges en lämplig säkerhetsnivå. Uppgifterna skall vara av sådan art att deras avslöjande skulle skada kommissionens eller medlemsstaternas intressen.

g) Inplacering i en lägre sekretessgrad innebär en sänkning av sekretessgraden.

h) Hävande av sekretess innebär att uppgifterna inte längre är hemligstämplade.

i) Upphovsman är författaren till ett sekretessbelagt dokument. Inom kommissionen får avdelningscheferna ge personalen tillstånd att stå som upphovsmän till sekretessbelagda EU-uppgifter.

j) Kommissionens tjänstegrenar är kommissionen och dess enheter, inklusive kanslierna, på alla platser där kommissionen har anställda, även Gemensamma forskningscentret, representationerna och kontoren i unionen samt delegationer i tredjeland.

4.3 **Sekretessklassning**

a) 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 och fall där sekretessbeläggningen inte är tillräcklig.

b) Systemet för sekretessklassning är det instrument som skall användas för att omsätta principerna i verkligheten; ett liknande system för sekretessklassning skall 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.

c) Ansvaret för sekretessklassningen ligger hos uppgifternas upphovsman.

d) Sekretessgraden skall endast grunda sig på uppgifternas innehåll.

e) Sekretessklassningen av en handling som helhet skall vara minst densamma som den del som fått den högsta sekretessgraden. Samlade uppgifter får dock ges en högre sekretessgrad än de enskilda uppgifter som ingår.

f) Uppgifter skall endast sekretessklassas när det är nödvändigt och under så lång tid som krävs.

4.4 **Syftet med säkerhetsåtgärderna**

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.

5. HUR SÄKERHETEN SKALL ORGANISERAS

5.1 **Gemensamma miniminormer**

Kommissionen skall se till att gemensamma miniminormer för säkerhet iakttas av alla mottagare av sekretessbelagda EU-uppgifter, inom institutionen och under dess befogenhet, dvs. alla avdelningar och 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.

Kommissionen får endast tillåta att sekretessbelagda EU-uppgifter vidarebefordras till organ utanför EU-institutionerna om dessa, vid hantering av sekretessbelagda EU-uppgifter, kan garantera att föreskrifter följs som minst motsvarar miniminormerna

5.2 **Organisation**

Inom kommissionen organiseras säkerheten på två nivåer:

a) För kommissionen som helhet finns kommissionens säkerhetsavdelning med dess ackrediteringsmyndighet för säkerhet som också fungerar som krypteringsmyndighet och Tempest-myndighet (kalibreringslaboratoriet för tester av spänningar i termisk, elektromagnetisk och fysikalisk utrustning), samt med INFOSEC-myndigheten (informationssäkerhet) och ett eller flera centrala register för sekretessbelagda EU-uppgifter. Varje sådant register förestås av en eller flera kontrolltjänstemän.

b) På kommissionens avdelningar vilar ansvaret hos en eller flera lokala säkerhetsansvariga, en eller flera säkerhetsansvariga för de centrala datasystemen, säkerhetsansvariga för de lokala datasystemen och de lokala registren för sekretessbelagda EU-uppgifter med en eller flera kontrolltjänstemän.

c) De centrala säkerhetsorganen kommer att ge ytterligare handledning till de lokala säkerhetsorganen.

6. SÄKERHET FÖR PERSONALEN

6.1 **Säkerhetsprövning av personal**

Alla personer som behöver ha tillgång till uppgifter som fått beteckningen EU CONFIDENTIAL 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 bedöma dessa personer i följande avseenden:

a) Om de är obrottsligt lojala.

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

c) Om de kan tänkas kunna påverkas av utländska eller andra källor.

Särskilt noggrann granskning inom ramen för säkerhetsprövningen skall göras av följande personer:

d) De som skall beviljas tillgång till uppgifter som klassats som EU TOP SECRET.

e) I tjänsteutövningen har de tillgång till en stor mängd uppgifter som berör EU på nivån EU SECRET.

f) Personer vars tjänsteutövning ger dem särskild tillgång till säkra kommunikations- eller informationssystem 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.

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.

6.2 **Register över säkerhetsprövning av personal**

Alla kommissionens avdelningar som hanterar sekretessbelagda EU-uppgifter eller där det finns säkra kommunikations- eller informationssystem, 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. Den lokale säkerhetsansvarige på kommissionen skall hålla ett register över säkerhetsprövningar inom sitt område.

6.3 **Säkerhetsanvisningar för personalen**

All personal, vars tjänst innebär att de kan få tillgång till sekretessbelagda uppgifter skall när de börjar sin tjänst och med regelbundna intervaller få en grundlig genomgång av kraven på säkerhet och hur denna säkerhet erhålls. Sådan personal skall skriftligen intyga att de tillfullo har läst och förstått dessa säkerhetsbestämmelser.

6.4 **Ledningsansvar**

Arbetsledningen skall ha skyldighet att känna till vilka av personalen som sysslar med sekretessbelagt arbete eller som har tillgång till skyddade kommunikations- eller informationssystem och registrera och rapportera incidenter eller uppenbart känsliga punkter som skulle kunna påverka säkerheten.

6.5 **Personalens säkerhetsstatus**

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 skyddade kommunikations- eller informationssystem, och att det berörda säkerhetskontoret på kommissionen 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.

7. FYSISK SÄKERHET

7.1 **Behov av skydd**

Den grad av fysiska säkerhetsåtgärder som skall tillämpas för att skydda sekretessbelagda EU-uppgifter skall stå i relation till den sekretessklassning, den volym och det hot som föreligger mot befintliga uppgifter och materiel. Alla som har tillgång till sekretessbelagda EU-uppgifter skall följa en gemensam praxis när det gäller sekretessklassning av dessa uppgifter och följa gemensamma skyddsnormer för hur uppgifter och materiel som kräver skydd skall förvaras, vidarebefordras/överföras och förstöras.

7.2 **Kontroller**

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.

7.3 **Byggnadernas säkerhet**

Byggnader där sekretessbelagda EU-uppgifter förvaras eller där det finns skyddade kommunikations- eller informationssystem, 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) sekretessklassningen 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.

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.

7.4 **Beredskapsplaner**

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

8. INFORMATIONSSÄKERHET

Informationssäkerheten rör fastställandet och tillämpningen av säkerhetsåtgärder för att skydda sekretessbelagda EU-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 sekretessbelagda EU-uppgifter, för att förhindra att behöriga användare nekas tillgång till sekretessbelagda EU-uppgifter och för att förhindra att sekretessbelagda EU-uppgifter förvanskas eller ändras eller raderas av obehöriga.

9. ÅTGÄRDER MOT SABOTAGE OCH ANDRA FORMER AV UPPSÅTLIG SKADA

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 ombedjas att samla in underrättelser om spionerі, sabotage, terrorism och annan omstörtande verksamhet.

10. UTLÄMNANDE AV SEKRETESSBELAGDA UPPGIFTER TILL TREDJELAND ELLER INTERNATIONELLA ORGANISATIONER

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

Om kommissionen erhåller sekretessbelagda uppgifter från tredjeland, internationella organisationer eller annan tredje part, skall dessa uppgifter skyddas i enlighet med den sekretessklassning 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.

Ovannämnda principer skall genomföras i enlighet med de detaljerade föreskrifterna i del II, avsnitt 26, och tilläggen 3, 4 och 5.

DEL II: SÄKERHETSORGANISATIONEN INOM KOMMISSIONEN

11. DEN LEDAMOT AV KOMMISSIONEN SOM ANSVARAR FÖR SÄKERHETSFRÅGOR

Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall utföra följande:

a) Genomföra kommissionens säkerhetspolitik.

b) Ta ställning till de säkerhetsproblem som kommissionen eller dess behöriga organ har hänskjutit till honom/henne.

c) Granska frågor som rör förändringar av kommissionens säkerhetspolitik, i nära samarbete med de nationella säkerhetsmyndigheterna (eller andra lämpliga organ) i medlemsstaterna (nedan kallade nationella säkerhetsmyndigheter).

Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall ansvara för följande:

a) Samordna alla säkerhetsärenden som rör kommissionens verksamhet.

b) Till de utsedda myndigheterna i medlemsstaterna översända ansökningar om att den nationella säkerhetsmyndigheten gör en säkerhetsprövning av personal som är anställd vid kommissionen, i enlighet med avsnitt 20.

c) Utreda eller begära en utredning om läckor av sekretessbelagda EU-uppgifter, som enligt prima facie-bevis har inträffat på kommissionen,

d) Begära att berörda säkerhetsmyndigheter inleder utredningar när man misstänker läckor av sekretessbelagda EU-uppgifter utanför kommissionen, och samordna utredningarna när mer än en säkerhetsmyndighet är inblandad,

e) Genomföra den periodiska inspektionen av säkerhetsarrangemangen för sekretessbelagda EU-uppgifter.

f) Stå i nära kontakt med alla berörda säkerhetsmyndigheter för att få till stånd en övergripande samordning av säkerheten.

g) Ständigt se över kommissionens säkerhetspolitik och säkerhetsförfaranden och, i förekommande fall, utarbeta lämpliga rekommendationer. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall i samband med detta för kommissionen lägga fram den årliga inspektionsplanen som utarbetas av kommissionens säkerhetstjänst.

12. KOMMISSIONENS RÅDGIVANDE KOMMITÉ FÖR SÄKERHETSFRÅGOR

En rådgivande kommitté för säkerhetsfrågor skall inrättas inom kommissionen. Den skall bestå av den ledamot för kommissionen som ansvarar för säkerhetsfrågor, eller dennes representant, som skall sitta som ordförande samt av representanter från varje medlemsstats nationella säkerhetsmyndighet. Representanter från andra Europeiska institutioner får också bjudas in att delta. Företrädare för decentraliserade EG och EU-myndigheter får också bjudas in att delta när frågor som rör dem diskuteras.

Kommissionens rådgivande kommitté för säkerhetsfrågor skall mötas när dess ordförande eller någon av dess medlemmar så begär. Kommittén skall ha till uppgift att granska och bedöma alla relevanta säkerhetsfrågor, samt att lägga fram rekommendationer till kommissionen när så behövs.

13. KOMMISSIONENS SÄKERHETSNÄMND

En säkerhetsnämnd skall inrättas inom kommissionen. Den skall bestå av generalsekreteraren som skall vara ordförande, och av generaldirektörerna för rättstjänsten, personal och administration, yttre förbindelser, rättsliga och inrikes frågor och gemensamma forskningscentret samt av cheferna för internrevisionen och kommissionens säkerhetstjänst. Andra kommissionstjänstemän får bjudas in. Dess ansvarsområde är att bedöma säkerhetsåtgärder inom kommissionen och att göra rekommendationer på detta område till den ledamot av kommissionen som ansvarar för säkerhetsfrågor.

14. KOMMISSIONENS SÄKERHETSKONTOR

För att uppfylla de skyldigheter som nämns i avsnitt 11 skall den ledamot av kommissionen som ansvarar för säkerhet kunna utnyttja kommissionens säkerhetstjänst för samordning, kontroll och genomförande av säkerhetsåtgärder.

Chefen för kommissionens säkerhetstjänst skall vara den främste rådgivaren till den ledamot av kommissionen som ansvarar för säkerhetsfrågor när det gäller sekretess, 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 kommissionen genom säkerhetsöverenskommelser. Han/hon skall i dessa avseenden agera som samordnare.

Chefen för kommissionens säkerhetstjänst skall ha ansvaret för godkännande av IT-system och IT-nät inom kommissionen. Chefen för kommissionens säkerhetstjänst skall tillsammans med relevant nationell säkerhetsmyndighet besluta om godkännande av IT-system och IT-nät som omfattar kommissionen och mottagare av sekretessbelagda EU-uppgifter.

15. SÄKERHETSSINSPEKTIONER

Återkommande inspektioner av säkerhetsanordningarna för insynsskydd av sekretessbelagda EU-uppgifter skall utföras av kommissionens säkerhetstjänst.

Kommissionens säkerhetstjänst får bistås i detta av säkerhetstjänster på andra EU-institutioner som innehar sekretessbelagda EU-uppgifter eller av medlemsstaternas nationella säkerhetsmyndigheter ([1]).

På begäran av en medlemsstat får en inspektion av sekretessbelagda EU-uppgifter utföras av dess nationella säkerhetsmyndighet inom kommissionen, gemensamt med kommissionens säkerhetstjänst och efter ömsesidig överenskommelse.

([1]) Utan att det påverkar Wienkonventionen från 1961 om diplomatiska förbindelser och Protokollet om Europeiska gemenskapernas immunitet och privilegier av den 8 april 1965.

16. KLASSNING< SÄKERHETSBETECKNINGAR OCH MÄRKNINGAR

16.1 **Klassningsnivåer ([1])**

Uppgifter kan placeras in i följande sekretessgrader (se även tillägg 2):

EU TOP SECRET: 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).

EU SECRET: 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).

EU CONFIDENTIAL: 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).

EU RESTRICTED: 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.

Inga andra klassningar är tillåtna.

16.2 **Säkerhetsbeteckningar**

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

Tilläggsmarkeringar, t.ex. CRYPTO eller någon annan säkerhetsbeteckning 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.

Säkerhetsbeteckningar skall endast användas tillsammans med en sekretessgrad.

16.3 **Märkningar**

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

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

Märkningen ESDP 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.

16.4 **Fastsättning**

Följande fastsättningsmetoder skall användas:

a) Handlingar med beteckningen EU RESTRICTED, på mekanisk eller elektronisk väg.

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

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

16.5 **Fastsättning av säkerhetsbeteckningar**

Säkerhetsbeteckningar skall sättas fast direkt under sekretessgraden och med samma metod.

([1]) Se den jämförande tabellen med sekretessgraderna inom EU, Nato, VEU och medlemsstaterna i bilaga 1.

17. HUR SEKRETESSKLASSNINGEN SKALL GÅ TILL

17.1 **Allmänt**

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

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

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

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.

Det antal personer som får författa dokument med beteckningen EU TOP SECRET skall vara så få som möjligt och deras namn skall finnas på en förteckning som upprättas av kommissionens säkerhetstjänst.

17.2 **Tillämpning av sekretessklassning**

Sekretessklassningen av en handling skall fastställas med utgångspunkt från hur känsligt handlingens innehåll är, i enlighet med definitionen i avsnitt 16. Det är viktigt att sekretessklassningen är korrekt och att den används med urskillning. Detta gäller särskilt säkerhetsgraden EU TOP SECRET.

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

En praktisk vägledning för sekretessklassning finns i bilaga 2.

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

Sekretessklassningen 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.

Allmänhetens tillgång till dokument skall även fortsättningsvis regleras genom förordning (EG) nr 1049/2001.

17.3 **Inplacering i lägre sekretessgrad och hävande av sekretess**

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. Upphovsmannen 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.

Upphovsmannen skall, om så är möjligt, på den sekretessbelagda handlingen ange ett datum, en tidsperiod eller en händelse 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 sekretessklassningen fortfarande är nödvändig.

18. FYSISK SÄKERHET

18.1 **Allmänt**

Det främsta syftet med de fysiska säkerhetsåtgärderna är att förhindra obehöriga från att få tillgång till sekretessbelagda EU-uppgifter eller materiel, förhindra stöld och förstörelse av utrustning och annan egendom samt förhindra trakasserier och andra typer av attacker mot personal, andra anställda och besökare.

18.2 **Säkerhetskrav**

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

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

a) sekretessklassningen av uppgifter 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.

De fysiska säkerhetsåtgärder som tillämpas skall

a) förhindra intrång i smyg eller genom tvång,

b) avskräcka, hindra och avslöja illojala personer,

c) hindra obehöriga från att få tillgång till sekretessbelagda EU-uppgifter.

18.3 **Fysiska säkerhetsåtgärder**

18.3.1 *Säkerhetsutrymmen*

Utrymmen där uppgifter med beteckningen EU CONFIDENTIAL 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 EU CONFIDENTIAL 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 sekretessklassningen 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 EU CONFIDENTIAL 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 EU CONFIDENTIAL 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.

18.3.2 *Administrativt utrymme*

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 EU RESTRICTED och uppgifter utan sekretessklassning skall hanteras och förvaras i administrativa utrymmen.

18.3.3 *Kontroll av in- och utpassering*

Tillträdet till och utgången från säkerhetsutrymmen av klass I och klass II skall kontrolleras genom passersedel eller genom att kontrollpersonalen känner igen personerna, vilket skall gälla för alla som normalt arbetar i dessa utrymmen. 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.

18.3.4 *Patrullering av vakter*

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.

18.3.5 *Säkerhetsskåp och valv*

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

— Klass A: säkerhetsskåp som godkänts nationellt för förvaring av uppgifter med beteckningen 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 EU och EU CONFIDENTIAL i ett säkerhetsutrymme av klass I eller klass II,

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

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

18.3.6 *Lås*

Lås som används för säkerhetsskåp och valv i vilka sekretessbelagda EU-uppgifter förvaras skall uppfylla 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.

18.3.7 *Kontroll av lås och kombinationer*

Nycklar till säkerhetsskåp får inte avlägsnas från kommissionens byggnader. Kombinationer till säkerhetsskåp skall memoreras av de personer som behöver känna till dem. För användning i nödsituationer skall den lokalt säkerhetsansvarige på kommissionsavdelningen 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 nycklar och kombinationer bör inte vara mindre strängt än de uppgifter som de ger tillgång till.

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.

18.3.8 *Anordningar för upptäckt av intrång*

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.

18.3.9 *Godkänd utrustning*

Kommissionens säkerhetstjänst skall hålla uppdaterade förteckningar över typer och modeller för den säkerhetsutrustning som den har godkänt för skydd av sekretessbelagda uppgifter under olika specificerade omständigheter och villkor. Kommissionens säkerhetstjänst skall basera dessa förteckningar bland annat på information från nationella säkerhetsmyndigheter.

18.3.10 *Fysiskt skydd för kopierings- och faxapparater*

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

18.4 **Skydd mot ”tjuvtittande” och ”tjuvlyssnande”**

18.4.1 *Tjuvtittande*

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

18.4.2 *Tjuvlyssnande*

Kontor eller utrymmen där sekretessbelagda EU-uppgifter med beteckningen EU SECRET eller högre regelbundet diskuteras skall skyddas mot passivt och aktivt tjuvlyssnande när hotbilden kräver det. Kommissionens säkerhetstjänst ansvarar för att bedöma riskerna för tjuvlyssnande, efter samråd med nationella säkerhetsmyndigheter, när så krävs.

18.4.3 *Införande av elektronisk utrustning och inspelningsutrustning*

Det är inte tillåtet att ta med mobiltelefoner, privata datorer, inspelningsutrustning, kameror och annan elektronisk utrustning eller inspelningsutrustning till säkerhetsutrymmen eller tekniska säkerhetsutrymmen utan tillstånd på förhand från chefen för kommissionens säkerhetstjänst.

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 kommissionens säkerhetstjänst begära hjälp av de nationella säkerhetsmyndigheterna.

När omständigheterna så kräver får telekommunikationsutrustning och elektrisk eller elektronisk kontorsutrustning av alla slag som används under möten på säkerhetsnivån EU SECRET och högre, kontrolleras av tekniska säkerhetsexperter från de nationella säkerhetsmyndigheterna på begäran av chefen för kommissionens säkerhetstjänst.

18.5 **Tekniska säkerhetsutrymmen**

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.

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 inte är tillåten utan tillstånd på förhand av relevant myndighet.

19. ALLMÄNNA REGLER OM PRINCIPEN FÖR BEHOV AV UPPGIFTER OCH SÄKERHETSGRANSKNING AV EU-PERSONAL

19.1 **Allmänt**

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

Ansvaret för att avgöra vem som behöver ta del av uppgifter skall ligga hos den avdelning där personen i fråga skall anställas.

Begäran om granskning av personal skall göras av avdelningarna.

Säkerhetsprövningen skall leda till att ett ”säkerhetsintyg för EU-personal” 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 EU-personal för en viss sekretessgrad kan ge innehavaren tillgång till uppgifter med lägre sekretessklassning.

Personer som inte är tjänstemän eller övriga anställda, t.ex. externa uppdragstagare, experter eller konsulter, 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.

Allmänhetens tillgång till dokument skall även fortsättningsvis regleras genom förordning (EG) nr 1049/2001.

19.2 **Särskilda regler om tillgång till uppgifter som klassats som EU TOP SECRET.**

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

Samtliga personer som behöver få tillgång till uppgifter med sekretessgraden EU TOP SECRET skall utses av den ledamot av kommissionen som ansvarar för säkerhet och deras namn skall införas i det register som är relevant för säkerhetsklassen EU TOP SECRET. Kommissionens säkerhetstjänst skall skapa och föra detta register.

Samtliga personer skall innan de får tillgång till uppgifter med sekretessgraden EU TOP SECRET underteckna en försäkran om att de informerats om kommissionens säkerhetsrutiner och att de till fullo är medvetna om sitt särskilda ansvar när det gäller att skydda uppgifter med sekretessgraden 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.

Om personer vid möten m.m. ges tillgång till information med sekretessgraden 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.

Samtliga personer som lämnar en tjänstgöring för vilken de har behövt tillgång till information med sekretessgraden EU TOP SECRET skall avföras från den lista som upprättats för säkerhetsklassen 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 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 EU TOP SECRET.

19.3 **Särskilda regler om tillgång till uppgifter som klassats som EU SECRET och EU CONFIDENTIAL.**

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

Samtliga personer som får tillgång till information med sekretessgraden EU SECRET eller EU CONFIDENTIAL skall vara förtrogna med om de aktuella säkerhetsbestämmelserna och skall vara medvetna om konsekvenserna vid försumlighet.

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

19.4 **Särskilda regler om tillgång till uppgifter som klassats som EU RESTRICTED.**

Personer med tillgång till uppgifter med sekretessgraden EU RESTRICTED skall göras uppmärksamma på de här säkerhetsbestämmelserna liksom påföljderna vid försumlighet.

19.5 **Förflyttningar**

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.

När en medarbetare förflyttas till en tjänst som innebär hantering av sekretessbelagt EU-material skall den lokale säkerhetsansvarige instruera honom/henne.

19.6 **Särskilda anvisningar**

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) försiktighetsåtgärder som de bör vidta i kontakter med pressen och företrädare för särskilda intressegrupper,

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 spionerі eller eventuella onormala förhållanden som kan ha relevans för säkerheten.

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.

Det finns inga säkerhetsbestämmelser inom kommissionen för privata resor till något som helst resmål för de personer som genomgått säkerhetsprövning för tillgång till sekretessbelagd EU-information. Kommissionens säkerhetstjänst 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.

20. FÖRFARANDE FÖR SÄKERHETSPRÖVNING FÖR KOMMISSIONSTJÄNSTEMÄN OCH ANDRA ANSTÄLLDA

a) Endast tjänstemän och andra anställda inom kommissionen eller personer som arbetar inom kommissionen, som på grund av sina åligganden och för sin tjänsteutövning behöver känna till eller använda sekretessbelagda uppgifter som innehas av kommissionen, skall ha tillgång till sådana uppgifter.

b) För att få tillgång till uppgifter med beteckningen EU TOP SECRET, EU SECRET OCH EU CONFIDENTIAL måste de personer som avses i punkt a ha givits behörighet i enlighet med det förfarande som avses i punkterna c och d i detta avsnitt.

c) Behörighet skall endast ges till personer som har genomgått säkerhetsprövning av de behöriga nationella myndigheterna i medlemsstaterna, i enlighet med förfarandet i punkterna i-n.

d) Chefen för kommissionens säkerhetstjänst skall ansvara för beviljande av sådan behörighet som avses i punkterna a, b och c.

e) Han/hon skall bevilja behörighet efter att ha erhållit yttrande från medlemsstaternas behöriga nationella myndigheter på grundval av den säkerhetsprövning som genomförts i enlighet med punkterna i-n.

f) Kommissionens säkerhetstjänst skall hålla en aktuell förteckning över alla känsliga tjänster, enligt uppgifter från kommissionens enheter, och över alla personer som givits (tillfällig) behörighet.

g) Behörigheten, som skall vara giltigt för en period av fem år, får inte ha längre varaktighet än de uppgifter på vars grundval det beviljades. Den får förnyas i enlighet med förfarandet i punkt e.

h) Behörigheten skall dras in av chefen för kommissionens säkerhetstjänst om han/hon anser att det är motiverat att göra så. Varje beslut att dra in behörighet skall meddelas dels den berörda personen, som kan komma att kallas in för samtal med chefen för kommissionens säkerhetstjänst, dels den behöriga nationella myndigheten.

i) Säkerhetsgranskningen skall genomföras med bistånd av den berörda personen och på begäran av chefen för kommissionens säkerhetstjänst. Den behöriga nationella myndigheten för granskning skall ligga i den medlemsstat där den person som skall få behörighet är medborgare. I de fall den berörda personen inte är medborgare i en EU-medlemsstat skall chefen för kommissionens säkerhetstjänst begära säkerhetsgranskningen från den EU-medlemsstat där personen är bosatt eller har varit bosatt en längre tid.

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

k) Chefen för kommissionens säkerhetstjänst 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 behörighet.

l) 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.

m) När medlemsstatens behöriga nationella myndigheter avger ett positivt yttrande får chefen för kommissionens säkerhetstjänst ge den berörda personen behörighet.

n) Ett negativt yttrande från de behöriga nationella myndigheterna skall meddelas den berörda personen som kan begära att få höras av chefen för kommissionens säkerhetstjänst. Om chefen för kommissionens säkerhetstjänst anser det nödvändigt får den anhålla hos de behöriga nationella myndigheterna om eventuella ytterligare förtydliganden. Om den negativa uppfattningen bekräftas skall behörighet inte beviljas.

o) Alla personer som beviljats behörighet enligt punkterna d och e skall, när behörigheten 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.

p) Chefen för kommissionens säkerhetstjänst skall vidta alla nödvändiga åtgärder för att genomföra detta avsnitt, bland annat när det gäller reglerna för tillgång till förteckningen över behöriga personer.

q) Chefen för kommissionens säkerhetstjänst 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 en tillfällig behörighet för en tidsperiod som inte får överstiga tre månader i avvaktan på resultatet av den undersökning som anges i punkt i.

r) Den preliminära och tillfälliga behörighet som utfärdas på detta sätt skall inte ge tillgång till uppgifter med beteckningen EU TOP SECRET; tillgång till sådana uppgifter skall begränsas till tjänstemän som verkligen har genomgått säkerhetsprövning med positivt resultat, i enlighet med punkt i. I avvaktan på resultatet av säkerhetsprövningen får de tjänstemän, för vilka det begärts behörighet på nivån EU TOP SECRET, tillfälligt och preliminärt ges tillstånd att få tillgång till uppgifter upp till och med nivån EU SECRET.

21. UPPRÄTTANDE, UTLÄMNANDE, ÖVERFÖRING, SÄKERHET I POSTHANTERINGEN SAMT EXTRA EXEMPLAR OCH ÖVERSÄTTNINGAR OCH UTDRAG UR SEKRETESSBELAGDA EU-HANDLINGAR

21.1 **Upprättande**

1. EU:s sekretessklassningar skall tillämpas enligt avsnitt 16 och som för EU CONFIDENTIAL och däröver 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 EU TOP SECRET och EU SECRET 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 EU CONFIDENTIAL eller högre sekretessgrad.

2. Handlingar med beteckningen EU CONFIDENTIAL 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.

3. De bestämmelser som reglerar datoriserad framställning av sekretessbelagda handlingar fastställs i avsnitt 25.

21.2 **Utlämnande**

1. Sekretessbelagda EU-uppgifter skall lämnas ut endast till personer som behöver känna till uppgifterna för sin tjänsteutövning och som har genomgått lämplig säkerhetsprövning. Upphovsmannen skall specificera det första utlämnandet.

2. Handlingar med beteckningen EU TOP SECRET skall passera genom registret för sådana handlingar (se avsnitt 22.2). När det gäller meddelanden med beteckningen EU TOP SECRET får det behöriga registret ge chefen för kommunikationscentrumet behörighet att framställa det antal kopior som specificeras i mottagarförteckningen.

3. Handlingar med beteckningen EU SECRET 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.

4. Alla handlingar med beteckningen EU CONFIDENTIAL och med högre sekretessgrad skall när de inkommer till eller lämnar ett generaldirektorat eller en tjänst registreras på avdelningen lokala register för sekretessbelagda EU-uppgifter. 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 (se avsnitt 22.1).

21.3 **Vidarebefordran/överföring av sekretessbelagda EU-handlingar**

21.3.1 *Förpackningar, kvitton*

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

2. Det inre kuvertet får endast öppnas av en kontrolltjänsteman vid registret (se avsnitt 22.1) 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 (se avsnitt 22.1) 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.

3. 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.

4. Innerkuvertet skall därpå placeras i ytterkuvertet, vilket måste ha ett försändelsenummer för att möjliggöra förfarandet med mottagningsbevis. Sekretessgraden får inte under några omständigheter anges på ytterkuvertet.

5. För handlingar med beteckningen EU CONFIDENTIAL eller med högre sekretessgrad skall kurirer och bud erhålla mottagningsbevis med angivande av försändelsenumren.

21.3.2 *Vidarebefordran inom en byggnad eller ett byggnadskomplex*

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.

21.3.3 *Överföring inom ett land*

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

2. När budföretag används för vidarebefordran av en handling med beteckningen 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 EU TOP SECRET ständigt står under direkt övervakning av en ansvarig tjänsteman.

3. Handlingar med beteckningen 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 EU TOP SECRET,

   b) transportsättet uppfyller nationella bestämmelser för vidarebefordran av handlingar med beteckningen EU TOP SECRET,

   c) tjänstemannen under inga omständigheter lämnar handlingar med beteckningen 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 EU TOP SECRET och som skall diarieföras och kontrolleras mot detta register när handlingarna återkommer.

4. Inom ett visst land får handlingar med beteckningarna EU SECRET och EU CONFIDENTIAL 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.

5. Kommissionens säkerhetstjänst kommer att på grundval av dessa bestämmelser utarbeta instruktioner för personal som medför sekretessbelagda EU-handlingar. 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 18,

   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.

21.3.4 *Överföring från ett land till ett annat*

1. Materiel med beteckningen EU CONFIDENTIAL eller högre sekretessgrad skall befordras från en medlemsstat till en annan med diplomat- eller militärkurir.

2. Personlig befordran av materiel med beteckningen EU SECRET och EU CONFIDENTIAL kan tillåtas om det sker på sådana villkor att det garanteras att de inte kan falla i händerna på någon obehörig.

3. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor får ge tillåtelse till personlig befordran 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 har brådskande behov av materielen. Kommissionens säkerhetstjänst bör utarbeta föreskrifter som omfattar personlig befordran på internationell nivå av sekretessbelagt materiel upp till och med beteckningen EU SECRET av personer som inte är diplomat- eller militärkurirer. Enligt föreskrifterna skall det krävas att

   a) budet har genomgått lämplig säkerhetsprövning,

   b) en lämplig avdelning eller ett 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-medlemsstater 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 18,

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.).

4. 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 ifrågasätts av tullen eller säkerhetstjänstemännen vid en flygplats.

21.3.5 *Vidarebefordran/överföring av handlingar med beteckningen EU RESTRICTED*

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

21.4 **Säkerhet när det gäller kurirer**

Alla kurirer och sändebud som anlitas för att befordra handlingar med beteckningarna EU SECRET och EU CONFIDENTIAL skall ha genomgått lämplig säkerhetsprövning.

21.5 **Teknisk överföring på elektronisk eller annan väg**

1. 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 25.

2. Endast godkända kommunikationscentrum och nät eller terminaler och system får överföra uppgifter med beteckningarna EU CONFIDENTIAL och EU SECRET.

21.6 **Extra exemplar och översättningar av utdrag från sekretessbelagda EU-handlingar**

1. Endast upphovsmannen får ge tillåtelse till kopiering eller översättning av handlingar med beteckningen EU TOP SECRET.

2. Om personer som inte genomgått säkerhetsprövning för sekretessgraden EU TOP SECRET behöver information som, trots att den finns i en handling med beteckningen EU TOP SECRET, inte har den sekretessgraden, får chefen för registret för handlingar med beteckningen EU TOP SECRET (se avsnitt 22.2) 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 sekretessgrad.

3. Handlingar med beteckningen EU SECRET eller lägre sekretessgrad får mångfaldigas och översättas av adressaten, inom ramen för dessa säkerhetsbestämmelser 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.

22. REGISTER FÖR SAMT GRANSKNING, KONTROLL, ARKIVERING OCH FÖRSTÖRING AV SEKRETESSBELAGDA EU-UPPGIFTER

22.1 **Lokala register för sekretessbelagda EU-uppgifter**

1. På varje avdelning inom kommissionen skall ett eller flera lokala register för sekretessbelagda EU-uppgifter ansvara för registrering, kopiering, sändning, arkivering och förstöring av handlingar med beteckningen EU SECRET och EU CONFIDENTIAL.

2. Om en avdelning inte har något lokalt register för sekretessbelagda EU-uppgifter får den använda sig av Generalsekretariatets lokala register för sekretessbelagda EU-uppgifter.

3. Lokala register för sekretessbelagda EU-uppgifter skall rapportera till den avdelningschef från vilken de får sina instruktioner. Chefen för dessa register skall vara kontrolltjänsteman för registret.

4. De skall övervakas av den lokalt säkerhetsansvarige när det gäller tillämpningen av bestämmelser om hantering av sekretessbelagda EU-handlingar och motsvarande säkerhetsåtgärder.

5. Tjänstemän som arbetar vid de lokala registren för de sekretessbelagda EU-uppgifterna skall vara behöriga att ha tillgång till uppgifterna i enlighet med avsnitt 20.

6. Under ledning av avdelningschefen skall de lokala registren för sekretessbelagda EU-uppgifter utföra följande:

   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.

7. Det lokala registret 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 avdelningen.

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

8. De allmänna reglerna i avsnitt 21 skall tillämpas på kommissionens lokala register för sekretessbelagda EU-uppgifter, om de inte ändras av de särskilda bestämmelser som fastställs i detta avsnitt.

22.2 **Registret för uppgifter med beteckningen EU TOP SECRET**

22.2.1 *Allmänt*

1. Ett centralt register för uppgifter med beteckningen EU TOP SECRET skall sköta registrering, hantering och distribution av handlingar med beteckningen EU TOP SECRET i enlighet med dessa säkerhetsbestämmelser. Chefen för registret med uppgifter som betecknas EU TOP SECRET skall vara kontrolltjänsteman för detta register.

2. Det centrala registret för uppgifter med beteckningen EU TOP SECRET kommer att vara den centrala myndigheten inom kommissionen för mottagande från och avsändning till andra EU-institutioner, medlemsstater, internationella organisationer och tredjeländer med vilka kommissionen har avtal 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 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 EU TOP SECRET skall inrättas enligt avsnitt 22.2.3 för att tillgodose långsiktiga behov och skall vara kopplade till ett centralt register för handlingar med beteckningen EU TOP SECRET. Om handlingar med beteckningen EU TOP SECRET behöver konsulteras temporärt får dessa handlingar lämnas ut utan att det inrättas någon underavdelning till ett register för handlingar med beteckningen EU TOP SECRET under förutsättning att det fastställs regler för att garantera att de fortfarande kontrolleras av ett lämpligt register för handlingar med beteckningen EU TOP SECRET och att alla fysiska och personalmässiga säkerhetsåtgärder iakttas.

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

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

22.2.2 *Centrala registret för uppgifter med beteckningen EU TOP SECRET*

I egenskap av kontrolltjänsteman skall chefen för det centrala registret för handlingar med beteckningen EU TOP SECRET ha ansvar för

a) att vidarebefordra/överföra handlingar med beteckningen EU TOP SECRET i enlighet med de bestämmelser som fastställs i avsnitt 21.3,

b) att upprätta en förteckning över alla underavdelningar till register för handlingar med beteckningen 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 EU TOP SECRET som distribuerats av det centrala registret,

d) att upprätta ett register över förvarade och distribuerade handlingar med beteckningen EU TOP SECRET,

e) att upprätta en uppdaterad förteckning över alla de centrala registren för handlingar med beteckningen 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 EU TOP SECRET i registret i enlighet med bestämmelserna i avsnitt 18.

22.2.3 *Underavdelningar till register för handlingar med beteckningen EU TOP SECRET*

I egenskap av kontrolltjänsteman skall chefen för underavdelningen till registret för handlingar med beteckningen EU TOP SECRET ha ansvar för

a) att vidarebefordra/överföra handlingar med beteckningen EU TOP SECRET i enlighet med de bestämmelser som fastställs i avsnitt 21.3,

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

c) att lämna ut handlingar med beteckningen 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 EU TOP SECRET som förvaras eller lämnas ut eller som har översänts till andra register för handlingar med beteckningen EU TOP SECRET och att förvara alla motsvarande mottagningsbevis,

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

f) att fysiskt skydda alla handlingar med beteckningen EU TOP SECRET i registret i enlighet med bestämmelserna i avsnitt 18.

22.3 **Inventeringar, granskning och kontroll av sekretessbelagda EU-handlingar**

1. Varje år skall varje register för EU TOP SECRET-uppgifter enligt detta avsnitt utföra en specificerad inventering av alla handlingar med beteckningen EU TOP SECRET. En handling anses falla under ett registers ansvar om registret fysiskt förvarar handlingen eller har ett mottagningsbevis från det register för handlingar med beteckningen 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. De skall lägga fram resultaten av de årliga inventeringarna för den ledamot av kommissionen som ansvarar för säkerhetsfrågor, senast den 1 april varje år.

2. Underavdelningar till register för EU TOP SECRET-handlingar 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.

3. EU-uppgifter med lägre sekretessgrad än EU TOP SECRET skall undergå interna kontroller enligt instruktioner från den ledamot av kommissionen som ansvarar för säkerhetsfrågor.

4. 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.

22.4 **Arkivering av sekretessbelagda EU-uppgifter**

1. Sekretessbelagda EU-uppgifter skall arkiveras enligt relevanta bestämmelser i avsnitt 18.

2. För att minimera förvaringsproblemen skall kontrolltjänstemännen vid alla register ha behörighet att mikrofilma handlingar med beteckningarna EU TOP SECRET, EU SECRET och EU CONFIDENTIAL 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 sekretessklassningsnivå,

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

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

   d) filmrullar eller annan typ av stöd endast innehåller handlingar med samma sekretessklassning, dvs. EU TOP SECRET, EU SECRET eller EU CONFIDENTIAL,

   e) mikrofilmning eller arkivering av en handling med beteckningen EU TOP SECRET eller EU SECRET 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 avsnitt 22.5 nedan.

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

22.5 **Förstöring av sekretessbelagda EU-handlingar**

1. 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 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 EU TOP SECRET och av den tjänsteman som bevittnar förstöringen. Dessa personer skall ha genomgått säkerhetsprövning för sekretessgraden 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 EU TOP SECRET, inklusive allt sekretessbelagt material från upprättandet av handlingar med beteckningen EU TOP SECRET, t.ex. dåliga kopior, arbetsutkast, maskinskrivna noter och disketter, skall förstöras under överinseende av en kontrolltjänsteman för sekretessgraden 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.

2. Handlingar med beteckningen EU SECRET skall förstöras av det register som ansvarar för dessa handlingar under överinseende av en person som genomgått säkerhetsprövning, med hjälp av en av de processer som beskrivs i punkt 1 c. Handlingar med beteckningen EU SECRET som förstörs skall förtecknas på undertecknade intyg om förstöring vilka skall bevaras av registret tillsammans med distributionslistorna under minst tre år.

3. Handlingar med beteckningen EU CONFIDENTIAL skall förstöras av det register som ansvarar för dessa handlingar under överinseende av en person som genomgått säkerhetsprövning, med hjälp av en av de processer som beskrivs i punkt 1 c. Förstöringen skall registreras i enlighet med instruktioner från den ledamot av kommissionen som ansvarar för säkerhetsfrågor.

4. Handlingar med beteckningen EU RESTRICTED skall förstöras av det register som ansvarar för sådana handlingar eller av användaren i enlighet med instruktioner från den ledamot av kommissionen som ansvarar för säkerhetsfrågor.

22.6 **Förstöring i en nödsituation**

1. Kommissionens avdelningar 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 utarbeta de föreskrifter som bedöms nödvändiga för att hindra sekretessbelagda EU-uppgifter från att falla i händerna på obehöriga.

2. Arrangemangen för att skydda eller förstöra materiel med beteckningarna EU SECRET och EU CONFIDENTIAL i en kris skall under inga omständigheter kunna inverka ogynnsamt på skyddet eller förstöringen av materiel med beteckningen EU TOP SECRET, inklusive krypteringsutrustning, vars behandling skall prioriteras framför alla andra uppgifter.

3. De åtgärder som skall vidtas för att skydda och förstöra krypteringsutrustning i en nödsituation skall omfattas av särskilda föreskrifter.

4. Instruktioner skall finnas på plats i ett förseglat kuvert. Det måste finnas utrustning för förstöring.

23. Säkerhetsåtgärder för särskilda möten utanför kommissionens lokaler vilka inbegriper sekretessbelagda EU-uppgifter

23.1 **Allmänt**

När kommissionsmöten eller andra viktiga möten äger rum utanför kommissionens lokaler 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 skydd av sekretessbelagda EU-uppgifter. Andra säkerhetsåtgärder kan komma att behöva planeras.

23.2 **Ansvar**

23.2.1 *Kommissionens säkerhetstjänst*

Kommissionens säkerhetstjänst skall samarbeta med medlemsstatens behöriga myndigheter i den medlemsstat där mötet hålls (värdmedlemsstaten) för att garantera säkerheten vid kommissionens möte eller andra viktiga möten samt säkerheten för delegaterna 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 kommissionens kommunikationssystem för mottagande och vidarebefordran av sekretessbelagda EU-meddelanden. Värdmedlemsstaten kommer även att vid behov ombedjas att tillhandahålla säkra telefonsystem.

Kommissionens säkerhetstjänst 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.

Varje delegation kommer att till varje möte anmodas att 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 kommissionens säkerhetstjänst.

23.2.2 *Säkerhetstjänsteman vid möten*

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 denne säkerhetstjänsteman vidtar skall i allmänhet gälla följande:

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

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

c) Ständig samordning med värdmedlemsstatens behöriga myndigheter och med kommissionens säkerhetstjänst.

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

23.3 **Säkerhetsåtgärder**

23.3.1 *Säkerhetsutrymmen*

Följande säkerhetsutrymmen bör inrättas:

a) Ett säkerhetsutrymme i klass II bestående av ett planeringsrum, kommissionens kontor och reproduktionsutrustning samt delegationernas kontor vid behov.

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

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

23.3.2 *Passersedel*

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.

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.

Förutom deltagare med besöksbrickor bör så få personer som möjligt ha tillträde till mötesplatsen. Mötets säkerhetstjänsteman skall endast på begäran av de nationella delegationerna ge dessa tillstånd att ta emot besökare. 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.

23.3.3 *Kontroll av foto- och AV-utrustning*

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.

23.3.4 *Kontroll av portföljer, bärbara datorer och paket*

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.

23.3.5 *Teknisk säkerhet*

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

23.3.6 *Delegationernas handlingar*

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.

23.3.7 *Säker förvaring av handlingar*

Om 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.

23.3.8 *Inspektion av kontor*

Mötets säkerhetstjänsteman bör se till att kommissionens 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/hon vidta erforderliga åtgärder.

23.3.9 *Bortskaffande av sekretessbelagt EU-material*

Allt material skall behandlas som sekretessbelagt och papperskorgar eller säckar bör överlämnas till kommissionen och delegationerna för bortskaffande. Kommissionen 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.

Vid mötets slut bör alla handlingar som kommissionen eller delegationerna förfogar över men inte längre önskar behandlas som makulatur. Det bör göras en noggrann genomsökning av kommissionens 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 22.5.

24. SEKRETESSBROTT OCH RÖJANDE AV SEKRETESSBELAGDA EU-UPPGIFTER

24.1 **Definitioner**

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

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.

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

24.2 **Rapportering om sekretessbrott**

Alla personer som får hantera sekretessbelagda EU-uppgifter skall ingående informeras om sitt ansvar på detta område. De skall omedelbart rapportera varje sekretessbrott som de får kännedom om.

När en lokal säkerhetstjänsteman eller mötets säkerhetstjänsteman upptäcker eller informeras om ett sekretessbrott som gäller sekretessbelagda EU-uppgifter eller förlust eller försvinnande av sekretessbelagt EU-materiel skall denne vidta lämpliga åtgärder för att

a) säkra bevis,

b) fastställa fakta,

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

d) förhindra att brottet upprepas,

e) informera lämpliga myndigheter om effekten av sekretessbrott.

I detta sammanhang skall följande uppgifter tillhandahållas:

i) En beskrivning av de relevanta uppgifterna, inklusive sekretessgrad, 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.

Det skall vara varje säkerhetsmyndighets ansvar att så snart som den har underrättats om att ett sekretessbrott kan ha inträffat, rapportera detta till kommissionens säkerhetstjänst.

De fall som gäller uppgifter med beteckningen EU RESTRICTED behöver rapporteras endast när de uppvisar ovanliga kännetecken.

När den ledamot som ansvarar för säkerhet 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 sekretessgraden hos 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.

Upphovsmyndigheten skall underrätta adressaterna och ge lämpliga föreskrifter.

24.3 **Rättsliga åtgärder**

Varje person som är ansvarig för röjande av sekretessbelagda EU-uppgifter skall underkastas disciplinära åtgärder enligt de relevanta reglerna och bestämmelserna, särskilt avdelning VI i tjänsteföreskrifterna. Sådana åtgärder skall inte påverka eventuella vidare rättsliga åtgärder.

På grundval av den rapport som nämns i avsnitt 24.2 skall den ledamot av kommissionen som ansvarar för säkerhetsfrågor i lämpliga fall vidta alla åtgärder som krävs för att underlätta för de behöriga nationella myndigheterna att inleda rättsliga förfaranden.

25. SKYDD FÖR SEKRETESSBELAGDA EU-UPPGIFTER SOM HANTERAS I IT- OCH KOMMUNIKATIONSSYSTEM

25.1 **Inledning**

25.1.1 *Allmänt*

Säkerhetsstrategin och säkerhetskraven skall tillämpas på alla kommunikations- och informationssystem och kommunikations- och informationsnät (nedan kallade system) i vilka EU-uppgifter med sekretessgraden EU CONFIDENTIAL och högre hanteras. De skall tillämpas som ett komplement till kommissionens beslut K (95) 1510 slutlig av den 23 november 1995 on the protection of informatics systems.

För system i vilka EU-uppgifter med sekretessgraden EU RESTRICTED hanteras krävs också säkerhetsåtgärder för att bevara dessa uppgifters sekretess. För alla system krävs säkerhetsåtgärder för att skydda okränkbarheten och tillgängligheten hos dessa system och de uppgifter de innehåller.

I den strategi för datasäkerhet som kommissionen tillämpar ingår följande:

— Den är integrerad i den allmänna säkerheten och utgör ett komplement till informationssäkerhet, personalsäkerhet och fysisk säkerhet.

— Det finns en ansvarsfördelning mellan ägare till tekniska system, ägare till sekretessbelagda EU-uppgifter som lagras eller behandlas i tekniska system, datasäkerhetsspecialister och -användare.

— Säkerhetsprinciper och säkerhetskrav finns beskrivna i varje datasystem.

— Dessa principer och krav godkänns av en för ändamålet utsedd myndighet.

— Hänsyn tas till de särskilda aspekter som utgör hot mot IT-utrymmet och som gör det sårbart.

25.1.2 *Hot mot systemen och systemens sårbarhet*

Ett hot kan definieras som en möjlighet att oavsiktligt eller avsiktligt äventyra 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.

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.

25.1.3 *Huvudsyftet med säkerhetsåtgärderna*

Huvudsyftet med de säkerhetsåtgärder som anges i detta avsnitt är att de skall ge skydd mot obehörigt röjande av sekretessbelagda EU-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 av kommissionens säkerhetstjänst tillsammans med lämpliga särskilda säkerhetsförfaranden och säkerhetstekniker som är särskilt utformade för varje system.

25.1.4 *Redovisning av systemspecifika säkerhetskrav*

För alla system som hanterar EU-uppgifter med sekretessgraderna EU CONFIDENTIAL och högre skall det krävas att en redovisning av systemspecifika säkerhetskrav utarbetas av ägaren till det tekniska systemet (TSO, se Avsnitt 25.3.4) och ägaren till uppgifterna (se Avsnitt 25.3.5), vid behov med indata och bistånd från projektpersonalen och kommissionens säkerhetstjänst (såsom myndigheten för informationssäkerhet -Infosec, se Avsnitt 25.3.3) samt med godkännande av ackrediteringsmyndigheten för säkerhet (SAA, se Avsnitt 25.3.2).

En redovisning av systemspecifika säkerhetskrav skall också krävas när ackrediteringsmyndigheten för säkerhet bedömer att tillgängligheten och okränkbarheten av EU-uppgifter med sekretessgraden EU RESTRICTED eller icke sekretessbelagda EU-uppgifter kan äventyras.

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.

25.1.5 *Säkra driftsformer*

Alla system som hanterar EU-uppgifter med sekretessgraden EU CONFIDENTIAL 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, och

c) Flernivå.

25.2 **Definitioner**

Med ackreditering skall 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.

Med säkerhetsansvarig för de centrala datasystemen (CISO) avses en tjänsteman inom en central IT-myndighet som samordnar och övervakar säkerhetsåtgärder inom centralt organiserade system.

Med certifiering avses utfärdande av ett formellt 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.

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:

Sådana åtgärder omfattar krypterings-, överförings- och sändningssäkerhet och omfattar också säkerhet när det gäller förfaranden, fysiska egenskaper, personal och handlingar samt datasäkerhet.

Med datasäkerhet (COMPUSEC) 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.

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.

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) De allmänna behovet 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 kategoriberäkningar för de uppgifter som hanteras i systemet.

Med utvärdering avses en för uppgiften lämpad 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.

Med ägaren till uppgifterna (IO) avses den myndighet (avdelningschef) som är ansvarig för att skapa, behandla och använda informationen, men även för att besluta om vem som skall ha tillträde till dessa uppgifter.

Med informationssäkerhet (INFOSEC) 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.

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

Anmärkning:

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

Med IT-nät avses en geografiskt spridd 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.

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 hålla en godtagbar skyddsnivå för sekretessbelagda uppgifter.

Med IT-system avses utrustning, metoder och förfaranden och, om så krävs, personal, som samlats och organiserats i syfte att bearbeta uppgifter.

Anmärkningar:

(1) Med detta skall avses en sammansättning av installationer 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 kan allmänt fastställas som de faktorer som kontrolleras av en enda TSO.

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

Ett IT-systems säkerhetsegenskaper omfattar alla funktioner, karakteristika och egenskaper hos maskinvara/fasta program/programvara, vidare 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.

Med säkerhetsansvarig för de lokala datasystemen (LISO) avses en tjänsteman inom en avdelning inom kommissionen som är ansvarig för att samordna och övervaka säkerhetsåtgärder inom sitt område.

Med driftsform för flernivåsäkerhet avses en driftsform där SAMTLIGA personer som har tillgång till systemet INTE har behörighet för uppgifter med den högsta sekretessgraden som hanteras i systemet och där SAMTLIGA som har tillgång till systemet INTE har ett allmänt behov av tillgång de uppgifter som hanteras i systemet.

Anmärkningar:

(1) Denna driftsform gör det möjligt att löpande hantera uppgifter med olika sekretessgrad och olika kategoribeteckning.

(2) Det faktum att samtliga personer inte har behörighet för uppgifter med den högsta sekretessgraden tillsammans med avsaknaden av ett allmänt behov av tillgång till uppgifterna visar att det behövs datasäkerhetsegenskaper som medger selektiv tillgång till samt separering av uppgifter i systemet.

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.

Med säkra driftsmetoder avses de förfaranden som utarbetas av ägaren till de tekniska systemen och enligt vilka det fastställs vilka principer för säkerhetsfrågor som skall gälla, vilka driftsmetoder som skall användas samt personalens ansvar.

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 SAMTLIGA som har tillgång till systemet INTE har ett allmänt behov av tillgång till de uppgifter som hanteras i systemet.

Anmärkningar:

(1) Avsaknaden av ett allmänt behov av tillgång till uppgifterna visar att det behövs datasäkerhetsegenskaper som medger selektiv tillgång till samt 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, till dess att annat beslut fattas, skyddas på det sätt som gäller för uppgifter med den högsta kategoribeteckning och sekretessgrad som hanteras, såvida det inte finns en etikettfunktionen med godtagbar tillförlitlighet.

Med en redovisning av systemspecifika säkerhetskrav avses en uttömmande och tydlig redogörelse för de säkerhetsprinciper som skall iakttas och de säkerhetskrav som måste uppfyllas. Den skall bygga på kommissionens 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.

Med ägaren till de tekniska systemen (TSO) avses den myndighet som är ansvarig för skapande, underhåll, drift och nedstängning av ett system.

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

25.3 **Ansvar för säkerhet**

25.3.1 *Allmänt*

I det rådgivande uppdrag som Kommissionens rådgivande kommitté för säkerhetsfrågor har och som definieras i Avsnitt 12 ingår också frågor om informationssäkerhet. Denna kommitté skall organisera sitt arbete så att den kan avge expertutlåtanden i dessa frågor.

Kommissionens säkerhetstjänst skall ha ansvar för att utfärda detaljerade bestämmelser för informationssäkerhet, baserade på bestämmelserna i detta kapitel.

Om det uppstår problem när det gäller säkerheten (incidenter, överträdelser osv.) skall Kommissionens säkerhetstjänst omedelbart vidta åtgärder.

Kommissionens säkerhetstjänst skall ha en enhet för informationssäkerhet.

25.3.2 *Ackrediteringsmyndigheten för säkerhet (SAA)*

Chefen för kommissionens säkerhetstjänst skall vara ackrediteringsmyndighet för säkerhet (SAA) för kommissionen. Ackrediteringsmyndigheten för säkerhet skall ha det allmänna ansvaret för säkerhet samt på de specialiserade områdena informationssäkerhet, krypteringssäkerhet och Tempest-säkerhet.

Ackrediteringsmyndigheten för säkerhet skall ansvara för att systemen överensstämmer med kommissionens säkerhetsstrategi. En av dess uppgifter skall vara att godkänna system för hantering i driftsmiljön av sekretessbelagda EU-uppgifter upp till en fastställd sekretessgrad.

Behörigheten för ackrediteringsmyndigheten för säkerhet vid kommissionen skall omfatta alla system som är i drift i kommissionens byggnader. Om en del komponenter i ett system omfattas av behörigheten för ackrediteringsmyndigheten för säkerhet vid kommissionen och andra komponenter omfattas av behörigheten för andra ackrediteringsmyndigheter för säkerhet, får alla berörda parter gemensamt utse en ackrediteringsstyrelse som skall samordnas av ackrediteringsmyndigheten för säkerhet vid kommissionen.

25.3.3 *INFOSEC-myndigheten*

Chefen för enheten för informationssäkerhet vid kommissionens säkerhetstjänst är kommissionens INFOSEC-myndighet. INFOSEC-myndigheten skall

— 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 samt med 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 och fortbildning om informationssäkerhet,

— avge tekniska utlåtanden vid utredningar om informationssäkerhetsrelaterade incidenter,

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

25.3.4 *Ägaren till de tekniska systemen (TSO)*

Ansvaret för införande och tillämpning av kontroller och särskilda säkerhetsegenskaper i ett system vilar på ägaren till det systemet, dvs ägaren till de tekniska systemen (TSO). För centralt ägda system skall en säkerhetsansvarig för de centrala datasystemen (CISO) utses. Om så är nödvändigt skall varje avdelning utse en säkerhetsansvarig för de lokala datasystemen (LISO). I TSO:s ansvar ingår att skapa säkra driftsmetoder och detta ansvar löper genom ett systems hela livscykel, från dess tillblivelse fram till dess avskaffande.

Ägaren till de tekniska systemen skall specificera vilka säkerhetsnormer och säkerhetsrutiner som systemets leverantör skall följa.

Ägaren till de tekniska systemen får när så är lämpligt delegera en del av sitt ansvar till den säkerhetsansvarige för de lokala datasystemen. En och samma person kan ha flera funktioner i fråga om informationssäkerhet.

25.3.5 *Ägaren till uppgifterna (IO)*

Ägaren till uppgifterna (IO) skall ansvara för sekretessbelagda EU-uppgifter (och andra uppgifter) som skall föras in, behandlas och produceras i tekniska system. Han skall definiera behörighetskraven till dessa uppgifter i systemen. Han kan delegera detta ansvar till en datachef eller en databaschef inom sitt område.

25.3.6 *Användare*

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

25.3.7 *INFOSEC-utbildning*

INFOSEC-utbildning och -fortbildning skall finnas tillgänglig för all personal som behöver detta.

25.4 **Icke-tekniska säkerhetsåtgärder**

25.4.1 *Säkerhetsprövning av personalen*

Användarna av systemet skall genomgå säkerhetsprövning och ha behov av 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 kommissionens förfaranden.

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

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.

I 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.

Ändringar av säkerhetsinställningarna inom ett system skall göras av minst två behöriga medlemmar av personalen som arbetar tillsammans.

25.4.2 *Fysisk säkerhet*

IT-utrymmen och separata utrymmen med terminaler/arbetsstationer (enligt definitionerna i Avsnitt 25.2) där EU-uppgifter med sekretessgraden EU CONFIDENTIAL och högre hanteras med hjälp av informationsteknik eller där åtkomst till sådana uppgifter är möjlig, skall efter omständigheterna fastställas som EU-säkerhetsutrymme av antingen klass I eller klass II.

25.4.3 *Kontroll av åtkomsten till ett system*

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.

När information och materiel för kontroll av åtkomst inte längre används för detta ändamål skall den förstöras i enlighet med Avsnitt 25.5.4.

25.5 **Tekniska säkerhetsåtgärder**

25.5.1 *Informationssäkerhet*

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.

Det skall åligga kommissionen och de personer inom denna som innehar information att bedöma problemen i samband med aggregering av enskilda uppgifter och de slutsatser som kan dras av sammanhörande delar, och utifrån detta avgöra om den samlade informationen bör ges en högre sekretessgrad eller inte.

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.

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.

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.

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 ackrediteringsmyndigheten för säkerhet (se 25.5.4).

25.5.2 *Kontroll av uppgifter och uppgifternas spårbarhet*

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

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.

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 och registrering av utdata. För EU-uppgifter med sekretessgraden SECRET EU och högre skall sådana förfaranden omfatta särskilda anvisningar för uppgifternas spårbarhet.

25.5.3 *Hantering och kontroll av flyttbara lagringsmedier för datorer*

Alla flyttbara lagringsmedier för datorer med sekretessgraden EU CONFIDENTIAL 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.

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.

25.5.4 *Hävande av sekretess och förstöring av lagringsmedier för datorer*

Lagringsmedier för datorer som använts för registrering av sekretessbelagda EU-uppgifter får inplaceras i lägre sekretessgrad eller kan få sekretessen hävd om ett förfarande som godkänts av ackrediteringsmyndigheten används.

Lagringsmedier för datorer som har innehållit EU-uppgifter med sekretessgraden EU TOP SECRET eller uppgifter av en särskild kategori kan inte få sekretessen hävd och återanvändas.

Om sekretessen inte kan hävas för lagringsmedier för datorer eller de inte är återanvändningsbara, skall de förstöras enligt ovannämnda förfarande.

25.5.5 *Kommunikationssäkerhet*

Krypteringsmyndigheten är chef för kommissionens säkerhetstjänst

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.

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 i dess egenskap av krypteringsmyndighet.

Sekretessen för EU-uppgifter med sekretessgraden EU SECRET och högre skall under överföringen skyddas genom krypteringsmetoder eller krypteringsprodukter som har godkänts av den ledamot av kommissionen som har ansvar för säkerhetsfrågor, efter samråd med Kommissionens rådgivande kommitté för säkerhetsfrågor. Sekretessen för EU-uppgifter med sekretessgraden EU CONFIDENTIAL och högre skall under överföringen skyddas genom krypteringsmetoder eller krypteringsprodukter som har godkänts av kommissionens krypteringsmyndighet, efter samråd med Kommissionens rådgivande kommitté för säkerhetsfrågor.

Närmare föreskrifter för överföring av sekretessbelagda EU-uppgifter skall anges i särskilda säkerhetsanvisningar som har godkänts av Kommissionens säkerhetstjänst, efter samråd med Kommissionens rådgivande kommitté för säkerhetsfrågor.

Under exceptionella operativa omständigheter får EU-uppgifter med sekretessgraderna EU RESTRICTED, EU CONFIDENTIAL och EU SECRET överföras i klartext under förutsättning att varje tillfälle är uttryckligen godkänt och registrerat i vederbörlig ordning av ägaren till uppgifterna. Sådana exceptionella omständigheter är följande:

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

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.

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.

25.5.6 *Installations- och strålningssäkerhet*

Den första installationen av systemen och eventuella större ändringar av dem skall utföras av installatörer som har genomgått säkerhetsprövning och som står 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.

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

Tempest-motåtgärderna skall ses över och godkännas av Tempest-myndigheten (se 25.3.2).

25.6 **Säkerhet under hantering**

25.6.1 *Säkra driftsmetoder (SecOPs)*

I de säkra driftsmetoderna (SecOPs) fastställs principerna för säkerhetsfrågor, vilka driftsmetoder som skall användas samt personalens ansvar. Ägaren till de tekniska systemen (TSO) skall ansvara för utarbetandet av säkra driftsmetoder.

25.6.2 *Skydd för programvara/konfigureringshantering*

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 skall kontrolleras med regelbundna mellanrum för att säkerställa deras okränkbarhet och konstatera att de fungerar korrekt.

Nya eller ändrade versioner av programvara skall inte användas för att hantering av sekretessbelagda EU-uppgifter förrän de har kontrollerats av ägaren till systemen.

25.6.3 *Kontroll av förekomst av skadliga programvaru- eller datavirus*

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

Alla lagringsmedier för datorer som kommer till kommissionens skall kontrolleras med avseende på eventuella skadliga programvaru- eller datavirus innan de börjar användas i ett system.

25.6.4 *Underhåll*

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.

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.

25.7 **Upphandling**

25.7.1 *Allmänt*

Alla säkerhetsprodukter som skall användas i systemet och som skall upphandlas skall antingen ha utvärderats och certifierats eller hålla på att utvärderas och certifieras av ett lämpligt utvärderings- eller certifieringsorgan i någon av EU:s medlemsstater på grundval av internationellt erkända kriterier (t.ex. de gemensamma kriterierna för utvärdering av informationsteknisk säkerhet, ISO 15408). Särskilda förfaranden krävs för att få godkännande från kommissionens rådgivande kommitté för upphandling och kontrakt (ACPC).

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

25.7.2 *Ackreditering*

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 kommissionen som andra organisationer skall kommissionen och de relevanta säkerhetsmyndigheterna inbördes komma överens om ackrediteringen.

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

25.7.3 *Utvärdering och certifiering*

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.

Kraven för utvärdering och certifiering skall ingå i systemplaneringen och vara tydligt angivna i redovisningen av systemspecifika säkerhetskrav.

Utvärderings- och certifieringsförfarandena skall utföras i enlighet med godkända riktlinjer av personal som är tekniskt kunnig, har genomgått lämplig säkerhetsprövning och agerar för ägaren till de tekniska systemen.

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

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

25.7.4 *Rutinkontroll av säkerhetsegenskaper för fortsatt ackreditering*

Ägaren till de tekniska systemen skall fastställa förfaranden för rutinkontroll för att säkerställa att systemets alla säkerhetsegenskaper är fortsatt giltiga.

De typer av förändringar som föranleder ny ackreditering eller som kräver 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 ägaren till de tekniska systemen 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.

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

25.8 **Tillfällig eller sporadisk användning**

25.8.1 *Säkerhet för mikrodatorer/persondatorer*

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.

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).

25.8.2 *Användning av privat IT-utrustning för officiellt arbete vid kommissionen*

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.

Privatägd maskinvara, programvara och media får inte införas till något klass 1- eller klass 2-område där sekretessbelagda EU-uppgifter hanteras, såvida det inte finns skriftligt tillstånd från chefen för kommissionens säkerhetsavdelning. Ett sådant tillstånd kan endast ges av tekniska skäl i undantagsfall.

25.8.3 *Användning av IT-utrustning som ägs av en entreprenör eller har tillhandahållits nationellt för officiellt arbete vid kommissionen*

Chefen för kommissionens säkerhetsavdelning kan tillåta användning av IT-utrustning och programvara som ägs av en entreprenör i organisationer som stödjer kommissionens arbete. Även användandet av IT-utrustning och programvara som tillhandahållits nationellt kan tillåtas; 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 ackrediteringsmyndigheten för säkerhet konsulteras så att de inslag i informationssäkerheten som är tillämpliga på användningen av denna utrustning beaktas och genomförs på korrekt sätt.

26. UTLÄMNANDE AV SEKTRETESSBELAGDA EU–UPPGIFTER TILL TREDJELAND ELLER INTERNATIONELLA ORGANISATIONER

26.1.1 *Principer för utlämnande av sekretessbelagda EU-uppgifter*

Kommissionen skall som kollegium besluta om utlämnande av sekretessbelagda EU-uppgifter till tredje land eller internationella organisationer 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.

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. Kommissionens rådgivande säkerhetskommitté skall avge ett tekniskt yttrande till kommissionen i denna fråga.

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 en garanti för att det skydd som kommissionen kräver kommer att tillhandahållas.

26.1.2 *Nivåer*

När kommissionen har beslutat att sekretessbelagda uppgifter får lämnas ut eller utväxlas med en given stat eller internationell organisation, skall den 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.

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.

Samarbetsnivån skall avgöra vilka förfaranden och säkerhetsföreskrifter som gäller, angivna i tillägg 3, 4 och 5.

26.1.3 *Säkerhetsavtal*

När kommissionen har beslutat att det föreligger ett ständigt eller långsiktigt behov av att utväxla sekretessbelagda uppgifter mellan kommissionen och tredje land eller andra internationella organisationer, skall den 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.

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 har sekretessgraden EU RESTRICTED eller lägre.

Utkast till avtal om säkerhetsförfaranden eller samförståndsavtal skall diskuteras inom kommissionens rådgivande säkerhetskommitté innan de läggs fram för kommissionen för beslut.

Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall begära allt nödvändigt stöd från medlemsstatens nationella säkerhetsmyndigheter för att säkerställa att de uppgifter som skall lämnas ut används och skyddas i enlighet med bestämmelserna i avtalen om säkerhetsförfaranden eller samförståndsavtalen.

Bilaga 1

JÄMFÖRELSE AV NATIONELLA SEKRETESSGRADER

EU-klassning	EU-TOP SECRET	EU-SECRET	EU-CONFIDENTIAL	EU RESTRICTED
NATO-klassificering (1)				
VEU-klassning	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratom-klassning (2)	EURATOM TOP Secret	EURATOM secret	EURATOM Confidential	EURATOM 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 (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grekland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spanien	Secreto	Reservado	Confidencial	Difusión limitada
Frankrike	Très Secret Défense (4)	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	Hemlig	Hemlig	Hemlig
Förenade kungariket	Top Secret	Secret	Confidential	Restricted

(1) NATO – överensstämmelse med NATO:s klassificeringsnivåer kommer att skapas när säkerhetsavtalet mellan kommissionen och NATO förhandlas fram.
(2) Euratom Förordning nummer 3 av den 31 juli 1958 om skydd av EURATOM:s skeretessbelagda uppgifter
(3) Tyskland: VS = Verschlußsache
(4) Frankrike: klassificeringen "Très Secret Défense", som omfattar prioriterade statliga angelägenheter, kan endast ändras efter tillstånd från premiärministern.

Bilaga 2

PRAKTISK HANDLEDNING FÖR SÄKERHETSKLASSNING

Denna handledning är vägledande och får inte tolkas på så sätt att den innebär ändringar av de väsentliga bestämmelserna i avsnitt 16, 17, 20 och 21.

Sekretessgrad	När	Vem	Fastsättning	Inplacering i lägre sekretessgrad/hävande av sekretess/förstöring	
				Vem	När
EU TOP SECRET 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 [16.1].	Sekretessbrott avseende tillgångar med sekretessgraden EU TOP SECRET skulle sannolikt — innebära en direkt risk för den inre stabiliteten i EU, en av dess medlemsstater eller ett vänligt sinnat land — orsaka synnerligen allvarlig skada för relationerna med vänligt sinnade stater — direkt innebära omfattande förluster av människoliv — orsaka synnerligen allvarlig skada för effektiviteten eller säkerheten hos medlemsstaters eller andra deltagers styrkor, eller för den fortsatta effektiviteten inom ytterst värdefull säkerhets- eller underrättelseverksamhet — orsaka allvarlig långvarig skada för EU:s eller medlemsstaters ekonomi.	Vederbörligen behöriga personer (upphovsmän), generaldirektörer, förvaltningschefer [17.1] Upphovsmannen skall ange ett datum, en period eller ett tillfälle då innehållet får inplaceras i lägre sekretessgrad eller då sekretessen får hävas [16.2]. I annat fall skall denne se över handlingarna minst vart femte år för att säkerställa att den ursprungliga sekretessgraden fortfarande är nödvändig [17.3].	Sekretessgraden EU TOP SECRET skall anges på handlingar som klassats som EU TOP SECRET, eventuellt tillsammans med en markering och/eller försvarsmärkningen -ESDP, på mekanisk väg och för hand [16.4, 16.5, 16.3]. EU:s sekretessgrader och säkerhetsmarkeringar skall anges centrerat i marginalen upptill och nedtill på varje sida och varje sida skall numreras. På varje handlaing skall ett referensnummer och ett datum anges. Detta referensnummer skall agnes 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. Samtliga bilagor skall förtecknas på första sidan [21.1].	Hävande av skeretess eller inplacering i lägre sekretessgrad är endast upphovsmannens ansvar, och denne skall informera de adressater till vilka han har skickat eller kopierat handlignen om sådana ändringar [17.3]. Handlingar med sekretessgraden EU TOP SECRET skall förstöras av det centrala registret eller underavdelningen av registret som ansvarar för dem. Varje förstörd handling skall förteckans i ett intyg över förstöring som undertecknas av kontrolltjänstemannen för sekretessgraden EU TOP SECRET och av den tjänsteman som bevittnar förstöringen. Dessa personer skall ha genomgått säkerhetsprövning för sekretessgraden EU TOP SECRET. Det skall göras en notering i registret om detta. Registret skall bevara intygen om förstöring, tillsammans med distributionslistorna under tio år [22.5].	Överskottskopior och handlingar som inte längre behövs skall förstöras [22.5]. Handlingar med skeretessgraden EU TOP SECRET, inklusive allt sekretessbelygt material från upprättandet av handligar med sekretessgraden EU TOP SECRET, t.ex. dåliga kopior, arbetsutkast, maskinskrivan noter och karbonpapper, skall förstöras under överinseende av en tjänsteman för skretessgraden 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 [22.5].

Sekretessgrad	När	Vem	Fastsättning	Inplacering i lägre sekretessgrad/hävande av sekretess/förstöring	
				Vem	När
EU SECRET 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 [16.1].	Sekretessbrott avseende tillgångar med sekretessgraden EU SECRET skulle sannolikt — skapa internationella spänningar — allvarligt skada relationerna med vänligt sinnade stater — direkt innebära att människoliv sätts i fara eller att den allmänna ordningen eller enskild säkerhet eller frihet lider allvarlig skada — orsaka allvaralig skada för effektiviteten eller säkerheten hos medlemsstaters eller andra deltagares styrkor, eller för den fortsatta effektiviteten inom mycket färdefull säkerhets- eller underrättelseverksamhet — orsaka betydande materiell skada för EU:s eller någon av dess medlemsstaters finansiella, monetära, ekonomiska eller handelsmässiga intressen.	Behöriga personer (upphovsmän), generaldirektörer, förvaltningschefer [17.1]. Upphovsmannen skall ange ett datum eller en period då innehållet får inplaceras i lägre sekretessgrad eller då sekretessen får hävas [16.2]. I annat fall skall denne se över handlingarna minst vart femte år för att säkerställa att den ursprungliga sekretessgraden fortfarande är nödvändig [17.3].	Sekretessgraden EU SECRET skall anges på handlingar som klassats som EU SECRET, eventuellt tillsammans med en säkerhetsbeteckning och/eller försvarsmärkningen- ESDP, på mekansik väg och för hand [16.4, 16.5, 16.3]. EU:s sekretessgrader och säkerhetsmarkeringar skall anges centretat i marginalen upptill och nedtill på varje sida och varje sida skall numreras. På varje handling skall ett referensnummer och ett datum anges. Detta referensnummer skall 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. Samtliga bilagor skall förtecknas på första sidan [21.1].	Hävande av sekretess eller inplacering i lägre sekretessgrad är endast upphovsmannens ansvar, och denne skall informera de adressater till vilka han har skickat eller kopierat handlingen om sådana ändringar [17.3]. Handlingar med sekretessgraden EU SECRET skall förstöras av det register som ansvarar för dem, under överinseende av en person som har genomgått säkerhetsprövning. Handlingar som klassats som EU SECRET och som förstörs skall förtecknas på undertecknade intyg om förstöring, vilka registret skall förvara tillsammans med distributionslistorna under minst tre år [22.5].	Överskottkopior och handligar som inte längre behövs skall förstöras [22.5]. Handlingar med sekretessgraden EU SECRET, inklusive allt sekretessbelagt material från upprättandet av handlingar med beteckningen EU SECRET, t.ex. 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 [22.5].

Sekretessgrad	När	Vem	Fastsättning	Inplacering i lägre sekretessgrad/hävande av sekretess/förstöring	
				Vem	När
EU CONFIDENTIAL Denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna skada Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen [16.1].	Sekretessbrott avseende tillgångar med sekretessgraden EU CONFIDENTIAL skulle sannolikt — i avsevärd utsträckning skada diplomatiska relationer, dvs. föranleda formella protester eller andra påföljder — skada enskild säkerhet eller frihet — orsaka skada för effektiviteten eller säkerheten hos medlemsstaters eller andra deltagares styrkor, eller för effektiviteten inom värdefull säkerhets- eller underrättelseverksamhet — avsevärt undergräva den finansiella bärkraftigheten hos större organisationer — hindra utredning, eller underlätta förövandet av, allvarlig brottslighet — i betydande utsträckning motverka EU:s eller medlemsstaters finansiella, monetära, ekonomiska eller handelsmässiga intressen — allvarligt hindra utvecklingen eller gneomförandet av betydande delar av EU:s politik — avsluta eller på annat sätt allvarligt störa betydande delar av EU:s verksamhet	Behöriga personer (upphovsmän), generaldirektörer, förvaltningschefer [17.1]. Upphovsmannen skall ange ett datum eller en period då innehållet får inplaceras i lägre sekretessgrad eller då sekretessen får hävas. I annat fall skall denne se över handlingarna minst vart femte år för att säkerställa att den ursprungliga sekretessgraden fortfarande är nödvändig [17.3].	Sekretessgraden EU CONFIDENTIAL skall anges på handlingar som klassts som EU CONFIDENTIAL, eventuellt tillsammans med en säkerhetsbeteckning och/eller försvarsmärkningen – ESDP, på mekansik väg och för hand eller genom tryck på förstämplat, registrerat papper [16.4, 16.5, 16.3]. EU:s sekrtessgrader 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. Samtliga bilagor skall förtecknas på fösta sidan [21.1].	Hävande av sekretess eller inplacering i lägre sekretessgrad är endast upphovsmannens ansvar, och denna skall informera de adressater till vilka han har skickat eller kopierat handlingen om sådana ändringar [17.3]. Handlingar med sekretessgraden EU CONFIDENTIAL skall förstöras av det register som ansvarar för dem, under överinseende av en person som har genomgått säkerhetsprövning. Förstöringen av handlingarna skall reigstreras i enlighet med nationella bestämmelser och, när det gäller kommissionen eller decentraliserade EU-myndigheter, i enlighet med ordförandens anvisningar [22.5].	Överskottskopior och handlingar som inte behövs skall förstöras [22.5]. Handlingar med skretessgraden EU CONFIDENTIAL, inklusive allt sekretessbelagt material från upprättandet av handlingar med beteckningen EU CONFIDENTIAL, t.ex. dåliga kopior, arbetsutkast, maskinskrivna noter och karbonpapper, skall förstöras genom att brännas, omvandlas till pappermassa, gå genom en dokumentförstörare eller på annat sätt reducers så att de är oigenkännliga och icke möjliga att återställa [22.5].

Sekretessgrad	När	Vem	Fastsättning	Inplacering i lägre skeretessgrad/hävande av sekretess/förstöring	
				Vem	När
EU RESTRICTED Denna sekretessgrad skall användas för uppgifter och materiel vilkas röjande utan tillstånd skulle kunna vara ofördelaktigt för Europeiska unionens eller en eller flera av dess medlemsstaters intressen [16.1].	Sekretessbrott avseende tillgångar med sekretessgraden EU RESTRICTED skulle sannolikt — ha en negativ inverkan på diplomatiska relationer — orsaka betydande problem för enskilda — göra det svårare att upprätthålla effektiviteten eller säkerheten hos medlemsstaternas eller andra deltagares styrkor — orsaka finansiella förluster eller underlätta oskäliga vinster eller fördelar för enskilda eller företag — bryta åtaganden om att låta information från tredje part förbli konfidentiell — bryta mot lagbestämmelser mot spridning av uppgifter — försvåra utredning, eller underlätta förövandet av, allvarlig brottslighet — innebära nackdelar för EU eller medlemsstater i förhandlingar om politik eller handel — hindra effektiv utveckling eller genomförande av EU:s politik — undergräva god styrning av EU och dess verksamhet	Behöriga personer (upphovsmän), generaldirektörer, förvaltningschefer [17.1]. Upphovsmannen skall ange ett datum, en period eller ett tillfälle då innehållet får inplaceras i lägre sekretessgrad eller då sekretessen får hävas [16.2]. I annat fall skall denne se över handlingarna minst vart femte år för att säkerställa att den ursprungliga sekretessgraden fortfarande är nödvändig [17.3].	Sekretessgraden EU RESTRICTED skall anges på handlingar som klassats som EU RESTRICTED, eventuellt tillsammans med en säkerhetsbeteckning och/eller försvarsmärkningen – ESDP, på mekanisk väg och för hand [16.4, 16.5, 16.3]. EU:s sekretessgrader och säkerhetsmarkeringar skall anges centrerat i marginalen upptill och nedtill på varje sida och varje sida skall numreras. På varje handling skall ett referensnummr och ett datum anges [21.1].	Hävande av sekretess eller inplacring i lägre sekretessgrad är endast upphovsmannens ansvar, och denne skall informera de adressater till vilka han har skickat eller kopierat handligen om sådana ändringar [17.3]. Handlingar med skeretessgraden EU RESTRICTED skall förstöras av det register som ansvarar för dem eller av användaren, i enlighet med ansvisningar från ordföranden [22.5].	Överskottskopior och handlingar som inte längre behövs skall förstöras [22.5].

Tillägg 3

Handledning för utlämnande av sekretessbelagda EU–uppgifter till tredje land eller internationella organisationer: Samarbete på nivå 1

RUTINER

1. Det är kommissionen som kollegium som har behörighet att lämna ut sekretessbelagda EU-uppgifter till länder som inte är medlemmar av Europeiska unionen eller till andra internationella organisationer vilkas säkerhetspolitik och säkerhetsbestämmelser är jämförbara med EU:s.

2. I avvaktan på att det ingås ett säkerhetsavtal är det den ledamot av kommissionen som ansvarar för säkerhetsfrågor som har behörighet att granska framställningar om att lämna ut sekretessbelagda EU-uppgifter.

3. Vid denna granskning skall han/hon
   — begära in yttrande från upphovsmännen till de sekretessbelagda EU-uppgifter som eventuellt skall lämnas ut,
   — 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 dessa säkerhetsbestämmelser,
   — begära in yttrande från kommissionens rådgivande kommitté för säkerhetsfrågor beträffande den tilltro som kan sättas till mottagarstaterna eller de internationella organisationerna.

4. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall överlämna framställan om överlämnande, tillsammans med yttrandet från kommissionens rådgivande kommitté för säkerhetsfrågor, till kommissionen för beslut.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

5. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall meddela mottagarstaterna eller de internationella organisationerna om kommissionens beslut att lämna ut sekretessbelagd EU-information.

6. 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 säkerhetsföreskrifterna 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 sekretessgraden EU CONFIDENTIAL eller högre 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 av handlingar

   a) De praktiska rutinerna för vidarebefordran av handlingar skall fastställas genom avtal. I avvaktan på att sådana avtal ingås gäller bestämmelserna i Avsnitt 21. I avtalet skall det i synnerhet specificeras till vilka register sekretessbelagda EU-uppgifter skall skickas.

   b) Om de sekretessbelagda uppgifter till vilkas utlämnande kommissionen ger tillstånd inbegriper handlingar med sekretessgraden EU TOP SECRET skall mottagarstaten eller den internationella organisationen inrätta ett centralt register för EU och vid behov underavdelningar. För dessa register skall det tillämpas bestämmelser som är strikt likvärdiga med bestämmelserna i Avsnitt 22 i dessa säkerhetsföreskrifter.

9. Registrering

   Så snart ett register mottar en EU-handling med sekretessgraden EU CONFIDENTIAL eller högre skall det diarieföra den inkomna handlingen i ett diarium som innehåller spalter för datum för mottagande, uppgifter om dokumentet (datum, referens- och kopienummer), dess sekretessgrad, 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 22 i dessa säkerhetsföreskrifter. Kopior av intygen om förstöring av handlingar med sekretessgrad EU SECRET och 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 EU CONFIDENTIAL och EU SECRET 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 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 kommissionens 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) Kommissionens säkerhetstjänst, 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 kommissionens säkerhetstjänst för att förhindra att det inträffade upprepas skall genomföras.

14. Inspektioner

Kommissionens säkerhetstjänst 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 4

Handledning för utlämnande av sekretessbelagda EU–uppgifter till tredje land eller internationella organisationer: Samarbete på nivå 2

RUTINER

1. Behörigheten 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 upphovsmannen. Behörigheten att lämna ut sekretessbelagda EU-uppgifter som upprättats inom kommissionen tillkommer kommissionen som kollegium.

2. I princip är rätten begränsad till information med sekretessgrad upp till och med EU SECRET; den omfattar inte sekretessbelagda uppgifter som skyddas av särskilda säkerhetsbeteckningar eller markeringar.

3. I avvaktan på att det ingås ett säkerhetsavtal är det den ledamot av kommissionen som ansvarar för säkerhetsfrågor som har behörighet att granska framställningar om att lämna ut sekretessbelagda EU-uppgifter.

4. Vid denna granskning skall han/hon
   — begära in yttrande från upphovsmännen till de sekretessbelagda EU-uppgifter som eventuellt skall lämnas ut,
   — ta de erforderliga kontakterna 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 sekretessgrader som tillämpas inom EU och den berörda staten eller organisationen,
   — anordna ett möte i kommissionens rådgivande kommitté för säkerhetsfrågor eller, vid behov med förenklat skriftligt förfarande, begära att medlemsstaternas nationella säkerhetsmyndigheter skall utverka ett utlåtande från kommissionens rådgivande kommitté för säkerhetsfrågor.

5. Utlåtandet från kommissionens rådgivande kommitté för säkerhetsfrågor 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 överförs (genom att man bibehåller alternativt stryker rubricering av EU:s sekretessgrader, särskilda markeringar m.m.).
   — Inplacering i lägre sekretessgrad eller hävande av sekretessen innan uppgifterna lämnas ut till de mottagande länderna eller internationella organisationerna.

6. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall överlämna framställan om överlämnande, tillsammans med yttrandet från kommissionens rådgivande kommitté för säkerhetsfrågor, till kommissionen för beslut.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

7. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall meddela mottagarstaterna eller de internationella organisationerna om kommissionens beslut att lämna ut sekretessbelagd EU-information och om de restriktioner som gäller.

8. 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 de bestämmelser som kommissionen fastställt.

9. Följande skyddsföreskrifter skall tillämpas såvida inte kommissionen efter det att det mottagit utlåtandet från kommissionens rådgivande kommitté för säkerhetsfrågor beslutar om ett särskilt förfarande för handhavandet av sekretessbelagda EU-handlingar (genom att man avlägsnar uppgifter om EU:s sekretessgrad, särskilda markeringar m.m.).

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

    c) Den nationella säkerhetsprövningen eller behörigheten skall för kännedom tillställas ordföranden.

11. Vidarebefordran av handlingar

De praktiska rutinerna för vidarebefordran av handlingar skall fastställas genom avtal. I avvaktan på att sådana avtal ingås gäller bestämmelserna i Avsnitt 21. I avtalet skall särskilt anges de register till vilka sekretessbelagda EU-uppgifter skall sändas och de exakta adresser till vilka handlingarna skall sändas samt vilket bud- eller kurirföretag som anlitas för att befordra den sekretessbelagda EU-informationen.

12. 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 kommissionen, 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.

13. Returnering av handlingar

När mottagaren returnerar en sekretessbelagd handling till kommissionen skall det förfarande tillämpas som anges i punkten ”Vidarebefordran av handlingar” ovan.

14. 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 med behörighet att hantera sekretessbelagd EU-information. Om kombinationslås används får kombinationen endast vara känd av de tjänstemän inom staten eller organisationen som har behörighet 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 EU CONFIDENTIAL eller högre utan att kommissionens säkerhetstjänst lämnat sitt medgivande.

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

15. 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.

16. 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 kommissionens säkerhetstjänst eller den nationella säkerhetsmyndigheten i den medlemsstat som tagit initiativet till att vidarebefordra handlingarna (med kopia till kommissionens säkerhetstjänst).

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.

17. Inspektioner

Kommissionens säkerhetstjänst 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.

18. 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

Handledning för utlämnande av sekretessbelagda EU–uppgifter till tredje land eller internationella organisationer: Samarbete på nivå 3

RUTINER

1. Kommissionen 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.

2. Behörigheten 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 upphovsmannen. Behörigheten att lämna ut sekretessbelagda EU-uppgifter som upprättats inom kommissionen tillkommer kommissionen som kollegium.

   I princip är rätten begränsad till information med sekretessgrad upp till och med EU SECRET; den omfattar inte sekretessbelagda uppgifter som skyddas av särskilda säkerhetsbeteckningar eller markeringar.

3. Kommissionen 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.

4. Om kommissionen ställer sig positiv skall den ledamot av kommissionen som ansvarar för säkerhetsfrågor
   — begära in yttrande från upphovsmännen till de sekretessbelagda EU-uppgifter som eventuellt skall lämnas ut,
   — anordna ett möte i kommissionens rådgivande kommitté för säkerhetsfrågor eller, vid behov med förenklat skriftligt förfarande, begära att medlemsstaternas nationella säkerhetsmyndigheter skall utverka utlåtande från kommissionens rådgivande kommitté för säkerhetsfrågor.

5. Utlåtandet från kommissionens rådgivande kommitté för säkerhetsfrågor skall ta upp följande punkter:

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

   b) Sekretessgraden på de uppgifter som eventuellt skall lämnas ut.

   c) Inplacering i lägre sekretessgrad eller hävande av sekretess innan uppgifterna lämnas ut.

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

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

6. 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. Kommissionens rådgivande kommitté för säkerhetsfrågor kan rekommendera
   — 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 av handlingarna.

7. Ordföranden skall vidarebefordra utlåtandet från kommissionens rådgivande kommitté för säkerhetsfrågor till kommissionen för beslut.

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

9. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall informera medlemsstaterna om vilken typ av uppgifter det rör sig om och deras sekretessgrad samt ange till vilka organisationer och länder uppgifterna får lämnas ut i enlighet med kommissionens beslut.

10. Kommissionens säkerhetstjänst skall vidta de åtgärder som behövs för att underlätta framtida skadebedömningar och översyn av rutinerna.

    Närhelst förutsättningarna för samarbete ändras skall kommissionen ompröva frågan.

SÄKERHETSBESTÄMMELSER SOM SKALL TILLÄMPAS AV MOTTAGARNA

11. Den ledamot av kommissionen som ansvarar för säkerhetsfrågor skall meddela mottagarstaterna eller de internationella organisationerna om kommissionens beslut att lämna ut sekretessbelagda EU-uppgifter och om de skyddsföreskrifter som föreslagits av kommissionens rådgivande kommitté för säkerhetsfrågor och godkänts av kommisionen.

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

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

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

13. Vidarebefordran av handlingar

a) De praktiska rutinerna för att vidarebefordra handlingar skall beslutas gemensamt av kommissionens säkerhetstjänst 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 EU CONFIDENTIAL 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.

14. Diarieföring vid ankomsten

Den mottagande statens nationella säkerhetsmyndighet eller det motsvarande organ i den staten som på sin regerings vägnar tar emot sekretessbelagda uppgifter som vidarebefordrats av kommissionen, eller säkerhetsavdelningen vid den mottagande internationella organisationen, skall upprätta ett särskilt register för att diarieföra sekretessbelagda EU-uppgifter efter hand som dessa 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.

15. Användning och skydd av sekretessbelagda uppgifter som lämnats ut

a) Uppgifter med sekretessgraden EU SECRET skall hanteras av särskilt utsedda tjänstemän som bemyndigats att ha tillgång till uppgifter med denna sekretessgrad. Dessa skall arkiveras i väl inrättade säkra förvaringsskåp, som endast kan öppnas av personer som bemyndigats att ha tillgång till de uppgifter som finns där. De utrymmen där dessa skåp 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 EU SECRET skall översändas med diplomatisk kurirförsändelse, säkra postföretag och säkra telekommunikationsmedel. En handling med sekretessgraden EU SECRET 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 EU SECRET.

b) Uppgifter med sekretessgraden EU CONFIDENTIAL 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 EU CONFIDENTIAL 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 EU RESTRICTED 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.

16. Förstöring

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

17. Sekretessbrott

Om uppgifter med sekretessgraden EU CONFIDENTIAL eller EU SECRET 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. Resultatet skall meddelas kommissionens säkerhetstjänst. Nödvändiga åtgärder skall vidtas för att rätta till bristfälliga rutiner eller arkiveringsmetoder om dessa legat till grund för läckan.

Tillägg 6

FÖRKORTNINGAR

ACPC	Advisory Committee on Procurement and Contracts (rådgivande kommitté för upphandling och avtal)
CrA	Crypto Authority (krypteringsmyndighet)
CISO	Central Informatics Security Officer (säkerhetsansvarig för de centrala datasystemen)
COMPUSEC	Computer Security (datorsäkerhet)
COMSEC	Communication Security (kommunikationssäkerhet)
CSO	Commission Security Office (kommissionens säkerhetsjänst)
ESDP	European Security and Defence Policy (euroepeiska säkerhets- och försvarspolitiken)
EUCI	EU classified information (sekretessbelagda EU-uppgifter)
IA	INFOSEC Authority (INFOSEC-myndigheten)
INFOSEC	Information Security (informationssäkerhet)
IO	Information Owner (ägaren till uppgifter)
ISO	International Organisation for Standardisation (internationella standardiseringsorganisationen)
IT	Information Technology (informationsteknologi)
LISO	Local Informatics Security Officer (säkerhetsansvarig för de lokala datasystemen)
LSO	Local Security Officer (lokal säkerhetsansvarig)
MSO	Meeting Security Officer (säkerhetstjänsteman vid möten)
NSA	National Security Authority (nationell säkerhetsmyndighet)
PC	Personal Computer (persondator)
RCO	Registry Control Officer (kontrolltjänsteman för registret)
SAA	Security Accreditation Authority (ackrediteringsmyndighet för säkerhet)
SecOPS	Security Operating Procedures (säkra dirftsmetoder)
SSRS	Specific Security Requirement Statement (redovisning av specifika säkerhetskrav)
TA	Tempest Authority (Tempest-myndighet)
TSO	Technical Systems Owner (ägaren till de tekniska systemen)