ISSN 1977-0820

Europeiska unionens officiella tidning

L 274

Svensk utgåva

Lagstiftning

femtiosjätte årgången

15 oktober 2013

Innehållsförteckning

Pris: 4 EUR

SV

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

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

II

(Icke-lagstiftningsakter)

BESLUT

RÅDETS BESLUT

av den 23 september 2013

om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter

(2013/488/EU)

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 240.3,

med beaktande av rådets beslut 2009/937/EU av den 1 december 2009 om antagande av rådets arbetsordning [1], särskilt artikel 24, och

av följande skäl:

(1) För att man ska kunna utveckla rådets verksamhet på alla områden som kräver hantering av säkerhetsskyddsklassificerade uppgifter bör ett övergripande säkerhetssystem för skydd av säkerhetsskyddsklassificerade uppgifter som omfattar rådet, dess generalsekretariat och medlemsstaterna inrättas.

(2) Detta beslut bör gälla där rådet, dess förberedande organ och rådets generalsekretariat hanterar säkerhetsskyddsklassificerade EU-uppgifter.

(3) I enlighet med nationella lagar och andra författningar, och i den utsträckning som krävs för rådets verksamhet, bör medlemsstaterna respektera detta beslut när deras behöriga myndigheter, personal eller entreprenörer hanterar säkerhetsskyddsklassificerade EU-uppgifter, så att de alla kan vara förvissade om att säkerhetsskyddsklassificerade EU-uppgifter ges en motsvarande skyddsnivå.

(4) Rådet, kommissionen och Europeiska utrikestjänsten (nedan kallad *utrikestjänsten*) är fast beslutna ett tillämpa likvärdiga säkerhetsnormer för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

(5) Rådet betonar vikten av att i tillämpliga fall låta Europaparlamentet och andra av unionens institutioner, organ, kontor eller byråer omfattas av de principer, normer och regler för skydd av säkerhetsskyddsklassificerade uppgifter som är nödvändiga för att skydda unionens och dess medlemsstaters intressen.

(6) Rådet bör fastställa en lämplig ram för utbyte av säkerhetsskyddsklassificerade EU-uppgifter som innehas av rådet med andra av unionens institutioner, organ, kontor eller byråer, i tillämpliga fall, i enlighet med detta beslut och gällande interinstitutionella arrangemang.

(7) Unionsorgan och -byråer som inrättats enligt avdelning V kapitel 2 i fördraget om Europeiska unionen (EU-fördraget), Europol och Eurojust bör inom ramen för sin interna organisation följa de grundläggande principer och miniminormer som fastställs i detta beslut för skydd av säkerhetsskyddsklassificerade EU-uppgifter, om så föreskrivs i den akt genom vilken de inrättats.

(8) Krishanteringsinsatser som fastställts enligt avdelning V kapitel 2 i EU-fördraget liksom den berörda personalen bör följa de säkerhetsbestämmelser som rådet antagit för att skydda säkerhetsskyddsklassificerade EU-uppgifter om så föreskrivs i den rådsakt genom vilken de inrättas.

(9) EU:s särskilda representanter och deras medarbetare bör följa de säkerhetsbestämmelser som rådet antagit för att skydda säkerhetsskyddsklassificerade EU-uppgifter om så föreskrivs i den relevanta rådsakten.

(10) Detta beslut påverkar inte artiklarna 15 och 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och tillhörande genomförandeinstrument.

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

[1] EUT L 325, 11.12.2009, s. 35.

(12) För att säkerhetsbestämmelserna för skydd av säkerhetsskyddsklassificerade EU-uppgifter ska börja tillämpas i tid för Republiken Kroatiens anslutning till Europeiska unionen bör detta beslut träda i kraft samma dag som det offentliggörs.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte, tillämpningsområde och definitioner

1. I detta beslut fastställs grundläggande principer och miniminormer för säkerhet för att skydda säkerhetsskyddsklassificerade EU-uppgifter.

2. Dessa grundläggande principer och miniminormer ska gälla för rådet och rådets generalsekretariat (*generalsekretariatet*) och iakttas av medlemsstaterna i enlighet med deras nationella lagar och andra författningar, så att de alla kan vara förvissade om att säkerhetsskyddsklassificerade EU-uppgifter ges en motsvarande skyddsnivå.

3. I detta beslut används de definitioner som anges i tillägg A.

Artikel 2

Definition av säkerhetsskyddsklassificerade EU-uppgifter, säkerhetsskyddsklassificering och säkerhetsskyddsmarkeringar

1. *Säkerhetsskyddsklassificerade EU-uppgifter*: uppgifter eller material som placerats på en EU-säkerhetsskyddsklassificeringsnivå och vars obehöriga röjande skulle kunna åsamka Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen olika grader av skada.

2. Säkerhetsskyddsklassificerade EU-uppgifter ska placeras in på en av följande säkerhetsskyddsklassificeringsnivåer:

a) TRÈS SECRET UE/EU TOP SECRET: uppgifter och material vars obehöriga röjande skulle kunna medföra synnerligt men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

b) SECRET UE/EU SECRET: uppgifter och material vars obehöriga röjande skulle kunna medföra betydande men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

c) CONFIDENTIEL UE/EU CONFIDENTIAL: uppgifter och material vars obehöriga röjande skulle kunna medföra ett inte obetydligt men för Europeiska unionens eller en eller flera medlemsstaters väsentliga intressen.

d) RESTREINT UE/EU RESTRICTED: uppgifter och material vars obehöriga röjande skulle kunna medföra endast ringa men för Europeiska unionens eller en eller flera medlemsstaters intressen.

3. Säkerhetsskyddsklassificerade EU-uppgifter ska förses med en säkerhetsskyddsmarkering i enlighet med punkt 2. De kan vara försedda med ytterligare markeringar för att ange vilket verksamhetsområde de avser, fastställa upphovsmannen, begränsa utlämning, begränsa användningen eller ange villkor för utlämnande.

Artikel 3

Regler för säkerhetsskyddsklassificeringen

1. De behöriga myndigheterna ska förvissa sig om att säkerhetsskyddsklassificerade EU-uppgifter placeras på en lämplig säkerhetsskyddsklassificeringsnivå, tydligt identifieras som säkerhetsskyddsklassificerade uppgifter och endast behåller sin säkerhetsskyddsklassificeringsnivå så länge som krävs.

2. Säkerhetsskyddsklassificerade EU-uppgifter får inte inplaceras på en lägre säkerhetsskyddsklassificeringsnivå och uppgifterna får inte upphöra att vara säkerhetsskyddsklassificerade, och inte heller får några av de markeringar som avses i artikel 2.3 ändras eller avlägsnas utan föregående skriftligt medgivande från upphovsmannen.

3. Rådet ska godkänna en säkerhetsstrategi för upprättande av säkerhetsskyddsklassificerade EU-uppgifter, som ska inbegripa en praktisk handbok om säkerhetsklassificering.

Artikel 4

Skydd av säkerhetsskyddsklassificerade uppgifter

1. Säkerhetsskyddsklassificerade EU-uppgifter ska skyddas i enlighet med detta beslut.

2. En innehavare av säkerhetsskyddsklassificerade EU-uppgifter ska vara ansvarig för att skydda dessa uppgifter i enlighet med detta beslut.

3. Om medlemsstaterna matar in säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsklassificering i unionens strukturer eller nät, ska rådet och generalsekretariatet skydda uppgifterna i enlighet med kraven för säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå i enlighet med jämförelsetabellen för säkerhetsskyddsklassificeringsnivåer i tillägg B.

4. En sammanställning av säkerhetsskyddsklassificerade EU-uppgifter kan motivera skydd på en nivå motsvarande en högre säkerhetsskyddsklassificeringsnivå än de enskilda ingående delarna.

Artikel 5

Hantering av säkerhetsrisker

1. De risker som de säkerhetsskyddsklassificerade EU-uppgifterna utsätts för ska hanteras som en process. Processen ska syfta till att identifiera kända säkerhetsrisker, fastställa säkerhetsåtgärder som ska minska riskerna till en acceptabel nivå i enlighet med de grundläggande principer och miniminormer som anges i detta beslut och till att tillämpa åtgärderna i enlighet med begreppet flernivåförsvar enligt definitionen i tillägg A. Åtgärdernas effektivitet ska utvärderas fortlöpande.

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

3. Kontinuitetsplaner ska beakta behovet att skydda säkerhetsskyddsklassificerade EU-uppgifter i krislägen för att förhindra obehörig tillgång eller röjande, eller att förlust av riktighet eller tillgänglighet går förlorad.

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

Artikel 6

Genomförande av detta beslut

1. När så krävs ska rådet på rekommendation av säkerhetskommittén godkänna säkerhetsstrategier där åtgärder för genomförande av detta beslut fastställs.

2. Säkerhetskommittén kan på sin nivå besluta om säkerhetsriktlinjer för att komplettera eller understödja detta beslut och olika slags säkerhetsstrategier som godkänts av rådet.

Artikel 7

Personalsäkerhet

1. Personalsäkerhet innebär tillämpning av åtgärder som ska garantera att tillgång till säkerhetsskyddsklassificerade EU-uppgifter endast beviljas personer

— som har behov av informationen för arbetet,

— som i förekommande fall har säkerhetsprövats för respektive säkerhetsskyddsklassificeringsnivå, och

— som har upplysts om sitt ansvar.

2. Förfarandena för personalsäkerhetsgodkännande ska utformas på ett sådant sätt att det kan fastställas om en person med beaktande av vederbörandes lojalitet, tillförlitlighet och pålitlighet kan få tillgång till säkerhetsskyddsklassificerad EU-information.

3. Alla de personer vid generalsekretariatet som för sina arbetsuppgifter behöver ha tillgång till eller hantera säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska säkerhetsprövas för respektive säkerhetsskyddsklassificeringsnivå innan de ges tillgång till sådana säkerhetsskyddsklassificerade EU-uppgifter. Dessa personer måste beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå och fram till ett visst datum av generalsekretariatets tillsättningsmyndighet.

4. Sådan personal från medlemsstaterna som avses i artikel 15.3, och som för sina arbetsuppgifter kan behöva ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, ska säkerhetsprövas för respektive säkerhetsskyddsklassificeringsnivå eller på annat sätt i kraft av sina arbetsuppgifter vederbörligen bemyndigas i enlighet med nationella lagar och andra författningar innan de beviljas tillgång till sådana säkerhetsskyddsklassificerade EU-uppgifter.

5. Alla ska, innan de ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter och därefter regelbundet, upplysas och vara medvetna om sitt ansvar att skydda säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut.

6. Genomförandebestämmelser för denna artikel fastställs i bilaga I.

Artikel 8

Fysisk säkerhet

1. Med fysisk säkerhet avses tillämpningen av fysiska och tekniska skyddsåtgärder för att hindra obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

2. Fysiska säkerhetsåtgärder ska vara utformade för att förhindra intrång i smyg eller genom tvång, avskräcka, hindra och avslöja otillåtna handlingar och möjliggöra olika behandling av personalen med avseende på deras tillgång till säkerhetsskyddsklassificerade EU-uppgifter utifrån principen om behovsenlig behörighet. Sådana åtgärder ska fastställas utifrån en riskhanteringsprocess.

3. Åtgärder för fysisk säkerhet ska införas i alla lokaler, byggnader, kontor, rum och andra utrymmen i vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras, inklusive utrymmen som inhyser de kommunikations- och informationssystem som avses i artikel 10.2.

4. Utrymmen där säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre förvaras ska fastställas som säkerhetsutrymmen i enlighet med bilaga II och godkännas av den behöriga säkerhetsmyndigheten.

5. Endast godkänd utrustning eller godkända anordningar ska användas för att skydda säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

6. Genomförandebestämmelser för denna artikel fastställs i bilaga II.

Artikel 9

Hantering av säkerhetsskyddsklassificerade uppgifter

1. Hanteringen av säkerhetsskyddsklassificerade uppgifter är tillämpning av administrativa åtgärder som avser att kontrollera säkerhetsskyddsklassificerade EU-uppgifter genom hela deras livscykel i syfte att komplettera åtgärder som anges i artiklarna 7, 8 och 10 och därigenom avskräcka och upptäcka avsiktlig eller oavsiktlig läcka eller förlust av dessa uppgifter. Sådana åtgärder gäller särskilt upprättande, registrering, kopiering, översättning, inplacering på en lägre säkerhetsskyddsklassificeringsnivå, beslut om att uppgifter inte längre ska vara säkerhetsskyddsklassificerade, befordran och förstöring av säkerhetsskyddsklassificerade EU-uppgifter.

2. Uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska registreras för säkerhetsändamål innan de lämnas ut och när de tas emot. De behöriga myndigheterna vid generalsekretariatet och i medlemsstaterna ska i detta syfte inrätta ett registreringssystem. Uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET ska registreras i de därför avsedda registren.

3. Enheter och utrymmen inom vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras ska inspekteras med jämna mellanrum av den behöriga säkerhetsmyndigheten.

4. Säkerhetsskyddsklassificerade EU-uppgifter ska transporteras mellan enheter och utrymmen utanför fysiskt skyddade områden på följande sätt:

a) Som allmän regel ska säkerhetsskyddsklassificerade EU-uppgifter överföras elektroniskt med kryptoprodukter som godkänts i enlighet med artikel 10.6.

b) Om produkterna i led a inte används, ska säkerhetsskyddsklassificerade EU-uppgifter överföras antingen

i) på elektroniska medier (t.ex. USB-minnen, cd-skivor, hårddiskar) som skyddas med kryptoprodukter som godkänts i enlighet med artikel 10.6, eller

ii) i alla övriga fall, som föreskrivet av den behöriga säkerhetsmyndigheten i enlighet med de relevanta skyddsåtgärderna i bilaga III.

5. Genomförandebestämmelser för denna artikel fastställs i bilagorna III och IV.

Artikel 10

Skydd av säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem

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

2. Med kommunikations- och informationssystem avses varje system som gör det möjligt att hantera information i elektronisk form. Ett kommunikations- och informationssystem ska innefatta alla de resurser som krävs för att det ska fungera, inklusive infrastruktur, organisation, personal och informationsresurser. Detta beslut ska tillämpas på kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter (*kommunikations- och informationssystem* eller *system*).

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

4. Samtliga kommunikations- och informationssystem ska genomgå en ackrediteringsprocess. Godkännandet från säkerhetssynpunkt ska syfta till att skapa förvissning om att alla lämpliga säkerhetsåtgärder har vidtagits och att tillräckligt hög skyddsnivå för de säkerhetsskyddsklassificerade EU-uppgifterna och systemen har uppnåtts i enlighet med detta beslut. I redovisningen av godkännandet från säkerhetssynpunkt ska fastställas högsta säkerhetsskyddsklassificeringsnivå för den information som får hanteras av ett system och motsvarande villkor.

5. Säkerhetsåtgärder ska genomföras för att skydda system som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre mot kompromettering av sådana uppgifter genom oavsiktliga elektromagnetiska läckor (*tempestsäkerhetsåtgärder*). Sådana säkerhetsåtgärder ska motsvara spridningsrisken och uppgifternas säkerhetsskyddsklassificeringsnivå.

6. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter, ska sådana produkter godkännas på följande sätt:

a) Konfidentialiteten för uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET och högre ska skyddas genom kryptoprodukter som har godkänts av rådet i egenskap av kryptogodkännande myndighet på rekommendation av säkerhetskommittén.

b) Konfidentialiteten för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED ska skyddas genom kryptoprodukter som har godkänts av rådets generalsekreterare (nedan kallad *generalsekreteraren*) i egenskap av kryptogodkännande myndighet på rekommendation av säkerhetskommittén.

Trots vad som sägs i led b får säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller RESTREINT UE/EU RESTRICTED inom medlemsstaternas nationella system skyddas genom kryptoprodukter som har godkänts av en medlemsstats kryptogodkännande myndighet.

7. När säkerhetsskyddsklassificerade EU-uppgifter överförs på elektronisk väg ska godkända kryptoprodukter användas. Trots detta krav får specifika förfaranden i krissituationer eller specifika tekniska konfigurationer enligt bilaga IV tillämpas.

8. Generalsekretariatets respektive medlemsstaternas behöriga myndigheter ska upprätta följande informationssäkringsfunktioner:

a) En myndighet för informationssäkring.

b) En tempestmyndighet.

c) En kryptogodkännande myndighet.

d) En kryptodistribuerande myndighet.

9. För varje system ska generalsekretariatets respektive medlemsstaternas behöriga myndigheter upprätta följande:

a) En ackrediteringsmyndighet för säkerhet.

b) En driftsansvarig myndighet för informationssäkring.

10. Genomförandebestämmelser för denna artikel fastställs i bilaga IV.

Artikel 11

Industrisäkerhet

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

2. Generalsekretariatet får genom kontrakt överlåta arbetsuppgifter som omfattar eller medför att säkerhetsskyddsklassificerade EU-uppgifter lämnas ut till, hanteras av eller förvaras av industrienheter eller andra enheter som är registrerade i en medlemsstat eller en tredjestat som har ingått ett avtal eller en administrativ överenskommelse enligt artikel 13.2 a eller b.

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

4. Den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig myndighet i varje medlemsstat ska så långt det är möjligt enligt nationella lagar och andra författningar säkerställa att entreprenörer och underentreprenörer som är registrerade på deras territorium vidtar alla lämpliga åtgärder för att skydda säkerhetsskyddsklassificerade EU-uppgifter under de förhandlingar som förs innan ett kontrakt ingås och när ett kontrakt som kräver säkerhetsskyddsavtal genomförs.

5. Den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig myndighet i respektive medlemsstat ska så långt det är möjligt enligt nationella lagar och andra författningar säkerställa att entreprenörer och underentreprenörer som är registrerade i den medlemsstaten och som deltar i entreprenader som kräver säkerhetsskyddsavtal eller underentreprenader som kräver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET inom sina anläggningar, antingen när de genomför sådana entreprenader eller innan kontraktet ingås, innehar ett säkerhetsskyddsgodkännande av verksamhetsställe på relevant säkerhetsskyddsklassificeringsnivå.

6. Entreprenörens eller underentreprenörens personal som för genomförandet av ett kontrakt som kräver säkerhetsskyddsavtal behöver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska beviljas ett personalsäkerhetsgodkännande av en nationell säkerhetsmyndighet, utsedd säkerhetsmyndighet eller någon annan behörig säkerhetsmyndighet i enlighet med nationella lagar och andra författningar samt de miniminormer som fastställs i bilaga I.

7. Genomförandebestämmelser för denna artikel fastställs i bilaga V.

Artikel 12

Utbyte av säkerhetsskyddsklassificerade EU-uppgifter

1. Rådet ska fastställa villkoren för utbyte av säkerhetsskyddsklassificerade EU-uppgifter som det innehar med andra av unionens institutioner, organ, kontor eller byråer. En lämplig ram får inrättas för detta, bland annat genom ingående av interinstitutionella avtal eller andra arrangemang när så krävs.

2. En sådan ram ska säkerställa att säkerhetsskyddsklassificerade EU-uppgifter skyddas på ett sätt som är lämpligt med avseende på deras säkerhetsskyddsklassificeringsnivå och enligt grundläggande principer och miniminormer som motsvarar dem som fastställs i detta beslut.

Artikel 13

Utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer

1. Om rådet fastställer att det finns ett behov av utbyte av säkerhetsskyddsklassificerade EU-uppgifter med en tredjestat eller internationell organisation, ska en lämplig ram fastställas för detta ändamål.

2. För att upprätta denna ram och fastställa ömsesidigt gällande bestämmelser om skydd av utbytta säkerhetsskyddsklassificerade uppgifter

a) ska unionen ingå avtal med tredjestater eller internationella organisationer om säkerhetsförfaranden för utbyte och skydd av säkerhetsskyddsklassificerade uppgifter (nedan kallade *informationssäkerhetsskyddsavtal*), eller

b) får generalsekreteraren på generalsekretariatets vägnar ingå administrativa överenskommelser i enlighet med punkt 17 i bilaga VI om säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som ska lämnas ut som en allmän regel inte är högre än RESTREINT UE/EU RESTRICTED.

3. Informationssäkerhetsavtal eller administrativa överenskommelser som avses i punkt 2 ska innehålla bestämmelser som sörjer för att säkerhetsskyddsklassificerade EU-uppgifter som tredjestater eller internationella organisationer får, skyddas på ett sätt som är lämpligt med avseende på deras säkerhetsskyddsklassificeringsnivå och enligt miniminormer som inte är mindre stränga än de som fastställs i detta beslut.

4. Beslutet att lämna ut säkerhetsskyddsklassificerade EU-uppgifter som upprättats i rådet till en tredjestat eller internationell organisation ska fattas av rådet i varje enskilt fall beroende på uppgifternas karaktär och innehåll, mottagarens behovsenliga behörighet och den fördel som unionen vinner därigenom. Om det inte är rådet som är upphovsman till de säkerhetsskyddsklassificerade uppgifterna, ska generalsekretariatet först söka skriftligt tillstånd av upphovsmannen. Om det inte går att fastställa vem denne är kommer rådet att ikläda sig detta ansvar.

5. Utvärderingsbesök ska anordnas för att utröna ändamålsenligheten i de säkerhetsåtgärder som tillämpas i en tredjestat eller internationell organisation för att skydda säkerhetsskyddsklassificerade EU-uppgifter som lämnas ut eller utbyts.

6. Genomförandebestämmelser för denna artikel fastställs i bilaga VI.

Artikel 14

Överträdelse av säkerhetsbestämmelserna och röjande av säkerhetsskyddsklassificerade EU-uppgifter

1. En överträdelse av säkerhetsbestämmelserna inträffar som resultat av en handling eller försummelse som begåtts av en person och som står i strid med säkerhetsbestämmelserna i detta beslut.

2. Röjande av säkerhetsskyddsklassificerade EU-uppgifter inträffar när dessa som resultat av ett säkerhetsbrott helt eller delvis har lämnats ut till obehöriga.

3. Överträdelser av säkerhetsbestämmelserna eller misstänkta överträdelser av säkerhetsbestämmelserna ska omedelbarts rapporteras till den behöriga säkerhetsmyndigheten.

4. Om det är känt eller om det föreligger rimliga skäl att anta att säkerhetsskyddsklassificerade EU-uppgifter har röjts eller förlorats, ska den nationella säkerhetsmyndigheten eller en annan behörig myndighet vidta alla lämpliga åtgärder i enlighet med tillämpliga lagar och andra författningar för att

a) underrätta upphovsmannen,

b) se till att personal som inte direkt berörs av brottet utreder ärendet för att fastställa fakta,

c) bedöma den potentiella skada som åsamkats unionens eller medlemsstaternas intressen,

d) vidta lämpliga åtgärder för att förhindra ett upprepande, och

e) underrätta lämpliga myndigheter om de vidtagna åtgärderna.

5. Den som är ansvarig för en överträdelse av säkerhetsbestämmelserna kan komma att underkastas disciplinära åtgärder enligt tillämpliga bestämmelser. Den som är ansvarig för röjande eller förlust av säkerhetsskyddsklassificerade EU-uppgifter ska underkastas disciplinära och/eller rättsliga åtgärder enligt tillämpliga lagar och andra författningar.

Artikel 15

Ansvar för genomförande

1. Rådet ska vidta alla åtgärder som är nödvändiga för att sörja för en övergripande enhetlig tillämpning av detta beslut.

2. Generalsekreteraren ska vidta alla nödvändiga åtgärder vid hantering eller förvar av säkerhetsskyddsklassificerade EU-uppgifter eller annan säkerhetsskyddsklassificerad information för att säkerställa att detta beslut tillämpas i utrymmen som används av rådet och inom generalsekretariatet av generalsekretariatets tjänstemän och övriga anställda, personal som har avdelats till generalsekretariatet och entreprenörer som anlitas av generalsekretariatet.

3. Medlemsstaterna ska vidta alla lämpliga åtgärder i enlighet med sina nationella lagar och andra författningar, för att säkerställa att detta beslut vid hantering eller förvar av säkerhetsskyddsklassificerade EU-uppgifter respekteras av

a) personal vid medlemsstaternas ständiga representationer vid Europeiska unionen och nationella delegater som deltar i rådsmöten eller i möten i rådets förberedande organ eller som deltar i annan rådsverksamhet,

b) annan personal vid medlemsstaternas nationella förvaltningar, även personal som avdelats till dessa förvaltningar, oavsett om de tjänstgör på medlemsstaternas territorium eller utomlands,

c) andra personer i medlemsstaterna som i kraft av sina arbetsuppgifter vederbörligen bemyndigats att ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter, och

d) entreprenörer som anlitas av medlemsstaterna, oavsett om de är verksamma på medlemsstaternas territorium eller utomlands.

Artikel 16

Säkerhetsorganisationen inom rådet

1. Som ett led i dess roll för att sörja för en övergripande enhetlig tillämpning av detta beslut ska rådet godkänna

a) de avtal som avses i artikel 13.2 a,

b) beslut om att tillåta eller godkänna utlämning av säkerhetsskyddsklassificerade uppgifter som upprättats eller innehas av rådet till tredjestater och internationella organisationer i enlighet med principen om upphovsmannens samtycke,

c) ett årligt program för utvärderingsbesök som rekommenderas av säkerhetskommittén för besök för att utvärdera medlemsstaternas enheter och utrymmen, unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer, och för utvärderingsbesök i tredjestater och vid internationella organisationer, för att utröna ändamålsenligheten i de åtgärder som genomförs för att skydda säkerhetsskyddsklassificerade EU-uppgifter, och

d) säkerhetsstrategier enligt artikel 6.1.

2. Generalsekreteraren ska fungera som generalsekretariatets säkerhetsmyndighet. I den egenskapen ska generalsekreteraren

a) genomföra rådets säkerhetsstrategi och se över den,

b) med medlemsstaternas nationella säkerhetsmyndigheter samordna alla säkerhetsfrågor som avser skyddet av säkerhetsskyddsklassificerade uppgifter som berör rådets verksamhet,

c) bevilja generalsekretariatets tjänstemän, övriga anställda och nationella experter behörighet för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, i enlighet med artikel 7.3,

d) i lämpliga fall beordra utredningar av eventuella inträffade eller misstänkta läckor eller förlust av säkerhetsskyddsklassificerade uppgifter som innehas av eller härrör från rådet och begära bistånd från de berörda säkerhetsmyndigheterna vid sådana utredningar,

e) periodiskt genomföra inspektion av säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade uppgifter i generalsekretariatets lokaler,

f) periodiskt genomföra besök för att utvärdera säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade EU-uppgifter vid unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer,

g) tillsammans och i samförstånd med berörda nationella säkerhetsmyndigheter periodiskt genomföra utvärderingar av säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade EU-uppgifter i medlemsstaternas enheter och utrymmen,

h) se till att säkerhetsåtgärder vid behov samordnas med medlemsstaternas behöriga myndigheter med ansvar för skyddet av säkerhetsskyddsklassificerade uppgifter, och i förekommande fall tredjestater eller internationella organisationer, bl.a. om arten av hoten mot säkerheten för säkerhetsskyddsklassificerade EU-uppgifter och vilka skyddsåtgärder som kan vidtas, och

i) ingå sådana administrativa överenskommelser som avses i artikel 13.2 b.

Generalsekretariatets säkerhetsavdelning ska stå till generalsekreterarens förfogande för bistånd inom detta ansvarsområde.

3. För tillämpningen av artikel 15.3 bör medlemsstaterna

a) utse en nationell säkerhetsmyndighet, enligt förteckningen i tillägg C, som ska ansvara för säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade EU-uppgifter, så att

i) säkerhetsskyddsklassificerade EU-uppgifter vid nationella ministerier, organ eller myndigheter, offentliga eller privata, inom landet eller utomlands, skyddas i enlighet med detta beslut,

ii) säkerhetsarrangemangen för skydd av säkerhetsskyddsklassificerade EU-uppgifter inspekteras eller utvärderas periodiskt,

iii) alla som är anställda vid en nationell förvaltning eller av en entreprenör som kan ges tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre har säkerhetsgodkänts på lämpligt sätt eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar,

iv) säkerhetsplaner upprättas vid behov för att minska risken att säkerhetsskyddsklassificerade EU-uppgifter röjs eller går förlorade,

v) säkerhetsfrågor som rör skydd av säkerhetsskyddsklassificerade EU-uppgifter samordnas med andra behöriga nationella myndigheter, inbegripet dem som avses i detta beslut, och

vi) svar ges på relevanta ansökningar om säkerhetsgodkännande från framför allt unionens organ, byråer, enheter och verksamheter som inrättats enligt avdelning V kapitel 2 i EU-fördraget samt EU:s särskilda representanter och deras medarbetare som tillämpar detta beslut eller dess principer;

b) se till att deras behöriga myndigheter lämnar information och råd till sina regeringar, och genom dem till rådet, om arten av hoten mot säkerheten när det gäller säkerhetsskyddsklassificerade EU-uppgifter och vilka skyddsåtgärder som kan vidtas.

Artikel 17

Säkerhetskommittén

1. En säkerhetskommitté inrättas härmed. Den ska granska och bedöma alla säkerhetsfrågor inom ramen för detta beslut och i lämpliga fall lämna rekommendationer till rådet.

2. Säkerhetskommittén ska bestå av företrädare för medlemsstaternas nationella säkerhetsmyndigheter; en företrädare för kommissionen och för Europeiska utrikestjänsten ska vara närvarande vid dess möten. Generalsekreteraren eller den företrädare som han utser ska vara ordförande. Kommittén ska sammanträda enligt anvisningar från rådet eller på begäran av generalsekreteraren eller en nationell säkerhetsmyndighet.

Företrädare för unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer får bjudas in att delta när frågor som rör dem diskuteras.

3. Säkerhetskommittén ska organisera sitt arbete så att den kan lämna rekommendationer inom särskilda områden som gäller säkerhet. Den ska inrätta en undergrupp med experter på informationssäkringsfrågor och vid behov andra undergrupper med experter. Den ska fastställa mandatet för sådana undergrupper med experter och ta emot deras verksamhetsrapporter och eventuellt rekommendationer till rådet.

Artikel 18

Ersättande av föregående beslut

1. Genom detta beslut upphävs och ersätts rådets beslut 2011/292/EU ([1]).

2. Alla säkerhetsskyddsklassificerade EU-uppgifter på en säkerhetsskyddsklassificeringsnivå enligt rådets beslut 2001/264/EG ([2]) och beslut 2011/292/EU ska även fortsättningsvis skyddas i enlighet med relevanta bestämmelser i det här beslutet.

Artikel 19

Ikraftträdande

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

Utfärdat i Bryssel den 23 september 2013.

På rådets vägnar

V. JUKNA

Ordförande

([1]) Rådets beslut 2011/292/EU av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 141, 27.5.2011, s. 17).

([2]) Rådets beslut 2001/264/EG av den 19 mars 2001 om antagande av rådets säkerhetsbestämmelser (EGT L 101, 11.4.2001, s. 1).

BILAGOR

BILAGA I

Personalsäkerhet

BILAGA II

Fysisk säkerhet

BILAGA III

Hantering av säkerhetsskyddsklassificerade uppgifter

BILAGA IV

Skydd av säkerhetsskyddsklassificerade EU-uppgifter som hanteras i kommunikations- och informationssystem

BILAGA V

Industrisäkerhet

BILAGA VI

Utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer

BILAGA I

PERSONALSÄKERHET

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 7. Den anger kriterier för att fastställa huruvida en person i fråga om lojalitet, tillförlitlighet och pålitlighet kan ges behörighet att ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter och vilka utredningsförfaranden och administrativa förfaranden som ska tillämpas för detta ändamål.

II. BEVILJANDE AV TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

2. En person får beviljas tillgång till säkerhetsskyddsklassificerade uppgifter när

a) personens behovsenliga behörighet fastställts,

b) personen har informerats om säkerhetsbestämmelserna och säkerhetsförfarandena för att skydda säkerhetsskyddsklassificerade EU-uppgifter och bekräftat sitt ansvar i fråga om skyddet av sådana uppgifter, och

c) för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre

— personen har beviljats personalsäkerhetsgodkännande för respektive nivå eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar, eller

— när det gäller generalsekretariatets tjänstemän, övriga anställda eller nationella experter, personen av generalsekretariatets tillsättningsmyndighet har getts behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå och fram till ett visst datum i enlighet med punkterna 16–25.

3. Varje medlemsstat och generalsekretariatet ska fastställa vilka befattningar i deras organisationer som kräver tillgång till uppgifter som placerats på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre och därför kräver säkerhetsgodkännande upp till respektive nivå.

III. KRAV FÖR PERSONALSÄKERHETSGODKÄNNANDE

4. Nationella säkerhetsmyndigheter eller andra behöriga nationella myndigheter ska, efter att ha mottagit en vederbörligen godkänd begäran, ansvara för att de av deras medborgare som behöver ha tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre säkerhetsprövas. Prövningsnormerna ska motsvara nationella lagar och andra författningar för att utfärda ett personalsäkerhetsgodkännande eller lämna en bedömning om att personen kan ges behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter, i förekommande fall.

5. Om den berörda personen är bosatt på en annan medlemsstats eller på en tredjestats territorium, ska de behöriga nationella myndigheterna begära bistånd från den behöriga myndigheten i bosättningsstaten i enlighet med nationella lagar och andra författningar. Medlemsstaterna ska bistå varandra med att genomföra säkerhetsutredningar i enlighet med nationella lagar och andra författningar.

6. Där så är möjligt enligt nationella lagar och andra författningar får nationella säkerhetsmyndigheter eller andra behöriga myndigheter göra en prövning av utländska medborgare som behöver ha tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre. Prövningsnormerna ska motsvara nationella lagar och andra författningar.

Kriterier för säkerhetsprövningen

7. En persons lojalitet, tillförlitlighet och pålitlighet för säkerhetsgodkännande för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska fastställas genom en säkerhetsprövning. Den behöriga nationella myndigheten ska göra en samlad bedömning med utgångspunkt i resultatet av en sådan prövning. Huvudkriterierna för detta är bland annat, om möjligt i enlighet med nationella lagar och andra författningar, att pröva om personen

a) har begått eller försökt begå, konspirerat med eller hjälpt och stött någon annan i syfte att i gärning utföra, spioneri, terrorhandling, sabotage, förräderi eller uppvigling,

b) har eller har haft samröre med spioner, terrorister, sabotörer eller personer som skäligen kan misstänkas vara sådana, eller haft samröre med företrädare för organisationer eller främmande stater, inklusive främmande staters underrättelsetjänster, som kan hota unionens och/eller medlemsstaternas säkerhet, såvida inte detta samröre bemyndigats som ett led i tjänsteutövningen,

c) är eller har varit medlem av en organisation som genom våldsamma, omstörtande eller andra olagliga medel strävar efter att bl.a. störta regeringen i en medlemsstat, ändra den konstitutionella ordningen i en medlemsstat eller förändra dess regeringsform eller regeringspolitik,

d) är eller har varit anhängare av en organisation enligt led c eller har eller haft nära samröre med medlemmar i sådana organisationer,

e) avsiktligen har undanhållit eller gett en vilseledande bild av eller förfalskat betydelsefulla uppgifter, i synnerhet sådana som rör säkerhetsfrågor, eller avsiktligen har ljugit vid ifyllandet av formuläret för säkerhetsprövning eller under en intervju i samband med en säkerhetsprövning,

f) har dömts för en straffbar gärning,

g) har en bakgrund präglad av alkoholberoende, narkotika- eller läkemedelsmissbruk,

h) är eller har varit inblandad i beteenden som kan leda till risk för utpressning eller påtryckningar,

i) i ord eller handling har visat prov på oärlighet, illojalitet, bristande tillförlitlighet eller opålitlighet,

j) allvarligt eller vid upprepade tillfällen har brutit mot säkerhetsföreskrifter, eller har försökt eller lyckats att vidta en otillåten åtgärd i fråga om kommunikations- och informationssystem, och

k) kan utsättas för påtryckningar (t.ex. genom att inneha en eller flera medborgarskap i länder utanför EU eller från släktingar eller närstående som kan vara sårbara för främmande underrättelsetjänsters verksamhet, terroristgrupper eller andra omstörtande organisationer eller personer vilkas syften kan hota unionens och/eller medlemsstaternas säkerhetsintressen).

8. När det är lämpligt, och i enlighet med nationella lagar och andra författningar, kan även en persons ekonomiska och medicinska bakgrund tas med i bedömningen i samband med säkerhetsprövningen.

9. I tillämpliga fall, och i överensstämmelse med nationella lagar och andra författningar, kan även makes eller makas, sambos eller nära familjemedlems beteende och situation anses av intresse i samband med säkerhetsprövningen.

Utredningskrav för tillgång till säkerhetsskyddsklassificerade EU-uppgifter

Inledande beviljande av ett säkerhetsgodkännande

10. Det inledande säkerhetsgodkännandet för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET ska grundas på en säkerhetsprövning som omfattar minst de senaste fem åren eller perioden från 18 års ålder fram till dagens datum, beroende på vilken period som är kortast, och som ska omfatta

a) ett ifyllt nationellt frågeformulär om personalsäkerhet för den sekretessgrad för säkerhetsskyddsklassificerade EU-uppgifter som personen kan behöva ha tillgång till; när frågeformuläret har fyllts i ska det översändas till den behöriga säkerhetsmyndigheten,

b) identitetskontroll/medborgarskap/nationalitet – personens födelsedatum, födelseort och identitet ska kontrolleras; personens medborgarskap och/eller nationalitet, tidigare och nuvarande, ska fastställas; detta ska omfatta en bedömning av eventuell mottaglighet för påtryckningar utifrån, till exempel på grund av tidigare hemvist eller tidigare kontakter, och

c) kontroll av nationella och lokala register – nationella säkerhetsregister och, om sådana finns, centrala brottsregister och/eller andra jämförbara myndighets- och polisregister ska kontrolleras. Polisregister med rättslig behörighet på den plats där personen har varit bosatt eller anställd ska kontrolleras.

11. Det inledande säkerhetsgodkännandet för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET ska grundas på en säkerhetsprövning omfattande minst de senaste tio åren, eller perioden från 18 års ålder fram till dagens datum, beroende på vilken period som är kortast. Om intervjuer genomförs enligt led e nedan ska undersökningarna omfatta minst sju år, eller perioden från 18 års ålder fram till dagens datum, beroende på vilken period som är kortast. Förutom de kriterier som anges i punkt 7 ovan ska följande sakförhållanden, så långt det är möjligt enligt nationella lagar och andra författningar, undersökas innan ett personalsäkerhetsgodkännande beviljas för TRÈS SECRET UE/EU TOP SECRET. De kan också undersökas innan ett sådant säkerhetsgodkännande beviljas för CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET PSC om detta fastställs i nationella lagar och andra författningar.

a) Ekonomisk ställning – uppgifter ska efterfrågas om personens ekonomi för att bedöma utsatthet för utländska eller inhemska påtryckningar på grund av allvarliga ekonomiska svårigheter eller för att upptäcka en oförklarligt hög levnadsstandard.

b) Utbildning – uppgifter ska efterfrågas för att kontrollera personens utbildningsbakgrund vid skolor, universitet och andra utbildningsanstalter där personen har studerat efter artonårsdagen eller under en lämplig period enligt den undersökande myndighetens bedömning.

c) Anställning – uppgifter om nuvarande och tidigare anställning ska inhämtas, grundade till exempelvis på arbetsintyg, skriftliga vitsord eller arbetsgivares eller arbetsledares synpunkter.

d) Militärtjänst – i förekommande fall ska personens tjänstgöring i de väpnade styrkorna och orsak till hemförlovning kontrolleras.

e) Intervjuer – om det föreskrivs och är tillåtet enligt nationell lag ska en eller flera intervjuer genomföras med personen. Intervjuer ska även genomföras med andra personer som kan göra en opartisk bedömning av den undersöktes bakgrund, verksamhet, lojalitet, tillförlitlighet och pålitlighet. Om det är nationell praxis att be den undersökte om referenser ska de som lämnar referenser intervjuas, såvida det inte finns goda skäl att inte göra det.

12. Kompletterande undersökningar ska genomföras vid behov och i enlighet med nationella lagar och andra författningar för att ta fram alla tillgängliga relevanta uppgifter om personen och för att bestyrka eller vederlägga negativa uppgifter.

Förnyelse av säkerhetsgodkännande

13. Efter det ursprungliga beviljandet av säkerhetsgodkännandet och under förutsättning att personen har haft oavbruten tjänst inom en nationell förvaltning eller vid generalsekretariatet och har ett fortsatt behov av tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ska säkerhetsgodkännandet granskas och förnyas minst vart femte år för ett godkännande som gäller TRÈS SECRET UE/EU TOP SECRET och vart tionde år för godkännanden som gäller SECRET UE/EU SECRET och CONFIDENTIEL UE/EU CONFIDENTIAL, med början från dagen för meddelandet om resultatet av den senaste säkerhetsprövning på vilken det grundas. Alla säkerhetsutredningar som gäller förnyelse av säkerhetsgodkännande ska omfatta hela perioden sedan den förra prövningen.

14. För förnyelse av säkerhetsgodkännande ska de faktorer som anges i punkterna 10 och 11 undersökas.

15. Begäran om förnyelse ska lämnas i god tid med tanke på den tid som krävs för säkerhetsprövningar. Om den berörda ansvariga nationella säkerhetsmyndigheten eller annan behörig nationell myndighet har mottagit den relevanta begäran om förnyelse med tillhörande frågeformulär om personalsäkerhet innan säkerhetsgodkännandet löper ut, och den nödvändiga säkerhetsprövningen inte har slutförts, får den behöriga nationella myndigheten trots det förlänga giltighetstiden för det befintliga säkerhetsgodkännandet med högst tolv månader om detta är tillåtet enligt nationella lagar och andra författningar. Om säkerhetsprövningen ännu inte har slutförts vid utgången av denna tolvmånadersperiod, ska personen tilldelas uppgifter som inte kräver säkerhetsgodkännande.

Förfaranden vid generalsekretariatet avseende behörigheter

16. För generalsekretariatets tjänstemän och övriga anställda ska generalsekretariatets säkerhetsmyndighet översända det ifyllda frågeformuläret om personalsäkerhet till den nationella säkerhetsmyndigheten i den medlemsstat där personen är medborgare med en begäran om att en säkerhetsprövning genomförs för den säkerhetsskyddsklassificeringsnivå för säkerhetsskyddsklassificerade EU-uppgifter som personen kommer att behöva ha tillgång till.

17. När generalsekretariatet får kännedom om information som är relevant för en säkerhetsprövning och som avser en person som har ansökt om ett säkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ska det i enlighet med tillämpliga bestämmelser meddela relevant nationell säkerhetsmyndighet detta.

18. Efter det att säkerhetsprövningen har slutförts, ska den relevanta nationella säkerhetsmyndigheten meddela generalsekretariatets säkerhetsmyndighet resultatet av prövningen med användning av det standardformat som säkerhetskommittén föreskriver för detta.

a) När säkerhetsprövningen leder fram till bedömningen att ingenting negativt är känt som skulle kunna ifrågasätta personens lojalitet, tillförlitlighet och pålitlighet, får generalsekretariatets tillsättningsmyndighet bevilja personen i fråga behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till respektive säkerhetsskyddsklassificeringsnivå till och med ett angivet datum.

b) När säkerhetsprövningen inte leder fram till en sådan positiv bedömning ska generalsekretariatets tillsättningsmyndighet meddela den berörda personen, som kan begära att bli hörd av tillsättningsmyndigheten. Tillsättningsmyndigheten får anhålla hos den behöriga nationella säkerhetsmyndigheten om eventuella ytterligare förtydliganden som enligt nationella lagar och andra författningar kan lämnas. Om resultatet bekräftas ska behörighet inte ges för tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

19. Säkerhetsprövningen, och de resultat som framkommit, ska omfattas av gällande relevanta lagar och andra författningar i den berörda medlemsstaten, även i fråga om överklagande. Beslut som har fattats av generalsekretariatets tillsättningsmyndighet ska kunna överklagas i enlighet med tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i Europeiska unionen, som fastställts i rådets förordning (EEG, Euratom, EKSG) nr 259/68 [1] (nedan kallade *tjänsteföreskrifterna och anställningsvillkoren*).

20. Nationella experter som har avdelats till generalsekretariatet för en tjänst som kräver tillgång till säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska för generalsekretariatets säkerhetsmyndighet uppvisa ett giltigt personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter innan de tillträder sin tjänst, utifrån vilket tillsättningsmyndigheten ska bevilja behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

21. Generalsekretariatet kommer att godta behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter som beviljats av någon annan av unionens institutioner, organ eller byråer, så länge denna fortfarande gäller. Behörigheten kommer att omfatta den berörda personens samtliga uppdrag inom generalsekretariatet. Den unionsinstitution, det unionsorgan eller den unionsbyrå där personen tillträder sin tjänst kommer att meddela relevant nationell säkerhetsmyndighet om bytet av arbetsgivare.

22. Om en persons tjänstgöringstid inte börjar inom tolv månader efter det att resultatet av säkerhetsprövningen meddelats generalsekretariatets tillsättningsmyndighet, eller om det uppstår ett avbrott på tolv månader i personens tjänstgöring, och vederbörande under tiden inte har varit anställd vid generalsekretariatet eller i en tjänst i någon medlemsstats nationella förvaltning, ska resultatet överlämnas till den berörda nationella säkerhetsmyndigheten för bekräftelse av att det fortfarande är giltigt och tillämpligt.

[1] Rådets förordning (EEG, Euratom, EKSG) nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper samt om införande av särskilda tillfälliga åtgärder beträffande kommissionens tjänstemän (EGT L 56, 4.3.1968, s. 1).

23. När generalsekretariatet får kännedom om en säkerhetsrisk som avser en person med behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ska det i enlighet med tillämpliga bestämmelser meddela detta till den relevanta nationella säkerhetsmyndigheten och får tillfälligt neka tillgång till säkerhetsskyddsklassificerade EU-uppgifter eller återkalla behörigheten för tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

24. Om en nationell säkerhetsmyndighet meddelar generalsekretariatet att det inte längre finns stöd för den positiva bedömning som gjorts i överensstämmelse med punkt 18 a av en person med behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter får generalsekretariatets tillsättningsmyndighet be den behöriga nationella säkerhetsmyndigheten om ytterligare klargöranden i överensstämmelse med nationella lagar och andra författningar. Om de negativa uppgifterna bekräftas ska behörigheten återkallas och personen ska uteslutas från tillgång till säkerhetsskyddsklassificerade EU-uppgifter och från tjänster där sådan tillgång är möjlig eller personen i fråga kan äventyra säkerheten.

25. Alla beslut om att återkalla eller tillfälligt upphäva behörigheten för tillgång till säkerhetsskyddsklassificerade EU-uppgifter för en tjänsteman eller annan anställd vid generalsekretariatet och i förekommande fall skälen till detta ska meddelas den berörda personen, som kan begära att bli hörd av tillsättningsmyndigheten. Information från en nationell säkerhetsmyndighet ska omfattas av gällande relevanta lagar och andra författningar i den berörda medlemsstaten, även i fråga om överklaganden. Beslut som har fattats av generalsekretariatets tillsättningsmyndighet ska kunna överklagas i enlighet med tjänsteföreskrifterna och anställningsvillkoren.

Register över säkerhetsgodkännanden och behörigheter

26. Register över personalsäkerhetsgodkännanden och behörigheter som beviljats för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska föras av varje medlemsstat respektive av generalsekretariatet. Dessa register ska åtminstone omfatta uppgifter om vilken säkerhetsskyddsklassificeringsnivå för EU-uppgifter personen kan få tillgång till, datum för utfärdandet av säkerhetsgodkännandet och dess giltighetstid.

27. Den behöriga säkerhetsmyndigheten får utfärda ett intyg om personalsäkerhetsgodkännande som visar vilken säkerhetsskyddsklassificeringsnivå för säkerhetsskyddsklassificerade EU-uppgifter som personen kan få tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), giltighetsdatum för relevant personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter eller behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter samt vilket datum själva intyget löper ut.

Undantag från kravet på personalsäkerhetsgodkännande

28. Tillgången till säkerhetsskyddsklassificerade EU-uppgifter för personer i medlemsstaterna som i kraft av sina arbetsuppgifter vederbörligen bemyndigats att ha tillgång till dessa ska fastställas i enlighet med nationella lagar och andra författningar. Dessa personer ska informeras om sina säkerhetsåligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

IV. SÄKERHETSUTBILDNING OCH MEDVETENHET

29. Alla personer som har beviljats ett säkerhetsgodkännande ska skriftligen bekräfta att de känner till sina åligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och följderna av läckor av säkerhetsskyddsklassificerade EU-uppgifter. Ett register över sådana skriftliga bekräftelser ska vid behov föras av medlemsstaten och av generalsekretariatet.

30. Alla som är behöriga att ha tillgång till eller som har till uppgift att hantera säkerhetsskyddsklassificerade EU-uppgifter ska inledningsvis göras medvetna om och regelbundet informeras om hot mot säkerheten, och de ska omedelbart rapportera misstänkta eller ovanliga kontakter eller aktiviteter till behöriga säkerhetsmyndigheter.

31. Alla som slutar en anställning för vilken det krävs tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska göras medvetna om och vid behov skriftligt bekräfta sina åligganden när det gäller det fortsatta skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

V. EXCEPTIONELLA OMSTÄNDIGHETER

32. Där så är möjligt enligt nationella lagar och andra författningar får ett säkerhetsgodkännande som en medlemsstats behöriga nationella myndighet har beviljat för tillgång till nationella säkerhetsskyddsklassificerade uppgifter tillfälligt, i avvaktan på ett personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ge nationella tjänstemän tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till motsvarande sekretessgrad enligt jämförelsetabellen i tillägg B, om en sådan tillfällig tillgång är nödvändig i unionens intresse. De nationella säkerhetsmyndigheterna ska informera säkerhetskommittén om en sådan tillfällig tillgång till säkerhetsskyddsklassificerade EU-uppgifter inte är möjlig enligt nationella lagar och andra författningar.

33. I brådskande fall får generalsekretariatets tillsättningsmyndighet, då detta är välmotiverat och i tjänstens intresse och i avvaktan på en fullständig säkerhetsprövning, efter samråd med den nationella säkerhetsmyndigheten i den medlemsstat där personen är medborgare och om inte annat följer av resultatet av de preliminära kontrollerna för att verifiera att inget negativt framkommit, ge generalsekretariatets tjänstemän och övriga anställda tillfällig behörighet att ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter för en viss funktion. Sådana tillfälliga personalsäkerhetstillstånd ska vara giltiga under högst sex månader och får inte medge tillgång till information på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET. Alla personer som har beviljats tillfälligt personalsäkerhetstillstånd ska skriftligen bekräfta att de känner till sina åligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och följderna vid läckor av säkerhetsskyddsklassificerade EU-uppgifter. Ett register över sådana skriftliga bekräftelser ska föras av generalsekretariatet.

34. När en person ska utnämnas till en tjänst för vilken det krävs ett säkerhetsgodkännande på en högre nivå än den personen för tillfället innehar, får utnämningen göras tillfällig under förutsättning att

a) ett tvingande behov av tillgång till säkerhetsskyddsklassificerade EU-uppgifter motiveras skriftligt av personens överordnade,

b) tillgången begränsas till de särskilda delar av säkerhetsskyddsklassificerade EU-uppgifter som krävs för uppdraget,

c) personen innehar ett giltigt personalsäkerhetsgodkännande eller behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter,

d) åtgärder har inletts för att få behörighet till tillgång på den nivå som krävs för tjänsten,

e) tillfredsställande kontroller har gjorts av den behöriga myndigheten av att personen inte allvarligt eller vid upprepade tillfällen har brutit mot säkerhetsbestämmelserna,

f) utnämningen av personen har godkänts av den behöriga myndigheten, och

g) en registrering av undantaget, inklusive en beskrivning av de uppgifter till vilka tillgången godkändes, ska göras av den enhet som ansvarar för registrering eller dess underenhet.

35. Ovannämnda förfarande ska användas för att vid ett enda tillfälle ge tillgång till säkerhetsskyddsklassificerade EU-uppgifter med högre säkerhetsskyddsklassificeringsnivå än den för vilken personen har säkerhetsprövats. Detta förfarande får inte upprepas.

36. Under ytterst exceptionella omständigheter, exempelvis uppdrag i fientliga miljöer eller under perioder av stigande internationell spänning, får medlemsstaterna och generalsekreteraren i nödfall, särskilt för att rädda liv, om möjligt skriftligt, bevilja tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET för personer som inte innehar det säkerhetsgodkännande som krävs, under förutsättning att ett sådant tillstånd är absolut nödvändigt och det inte finns några rimliga tvivel beträffande personens lojalitet, tillförlitlighet och pålitlighet. Detta tillstånd ska registreras med en beskrivning av de uppgifter till vilka tillgång har godkänts.

37. När det gäller uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET ska denna nödfallstillgång endast beviljas unionsmedborgare med behörighet att ha tillgång till antingen den nationella motsvarigheten till uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller till SECRET UE/EU SECRET.

38. Säkerhetskommittén ska informeras om när förfarandet i punkterna 36 och 37 tillämpas.

39. När lagar och andra författningar i en medlemsstat föreskriver strängare regler i fråga om tillfälliga tillstånd, tillfälliga uppdrag, enstaka tillgång eller nödfallstillgång till säkerhetsskyddsklassificerade uppgifter får förfarandet i detta avsnitt endast tillämpas inom ramen för de begränsningar som anges i tillämpliga nationella lagar och andra författningar.

40. Säkerhetskommittén ska få en årlig rapport om användningen av de förfaranden som anges i detta avsnitt.

VI. NÄRVARO VID MÖTEN I RÅDET

41. Om inte annat följer av punkt 28 får personer som ska delta i möten i rådet eller dess förberedande organ när uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre diskuteras endast göra detta efter bekräftelse på att de har intyg om säkerhetsgodkännande. För delegater ska ett intyg om personalsäkerhetsgodkännande eller annat bevis på säkerhetsgodkännande lämnas av den behöriga nationella myndigheten till rådets säkerhetsavdelning eller i undantagsfall överlämnas av den berörda delegaten personligen. I tillämpliga fall får en konsoliderad namnförteckning användas där säkerhetsgodkännandet styrks på lämpligt sätt.

42. Om ett personalsäkerhetsgodkännande av säkerhetsskäl återkallas för en person vars arbetsuppgifter kräver närvaro vid möten i rådet eller i dess förberedande organ, ska den behöriga myndigheten informera generalsekretariatet om detta.

VII. POTENTIELL TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

43. Kurirer, vakter och ledsagare ska säkerhetsprövas för respektive sekretessnivå eller prövade på annat lämpligt sätt i enlighet med nationella lagar och andra författningar samt informeras om säkerhetsförfaranden för skyddet av säkerhetsskyddsklassificerade EU-uppgifter och om sina åligganden att skydda den information som de har anförtrotts.

BILAGA II

FYSISK SÄKERHET

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 8. Här fastställs minimikrav för fysiskt skydd av lokaler, byggnader, kontor, rum och andra utrymmen där säkerhetsskyddsklassificerade EU-uppgifter hanteras och förvaras, inklusive utrymmen där kommunikations- och informationssystem förvaras.

2. Fysiska säkerhetsåtgärder ska utformas för att hindra obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter genom att man

   a) ser till att säkerhetsskyddsklassificerade EU-uppgifter hanteras och förvaras på lämpligt sätt,

   b) möjliggör olika behandling av personalen med avseende på tillgången till säkerhetsskyddsklassificerade EU-uppgifter på grundval av principen om behovsenlig behörighet och, där så är lämpligt, säkerhetsprövning,

   c) avskräcker, hindrar och avslöjar otillåtna handlingar, och

   d) förhindrar och försenar intrång i smyg eller genom tvång.

II. FYSISKA SÄKERHETSKRAV OCH SÄKERHETSÅTGÄRDER

3. Fysiska säkerhetsåtgärder ska väljas på grundval av en hotbedömning gjord av de behöriga myndigheterna. Generalsekretariatet och medlemsstaterna ska var för sig tillämpa ett riskhanteringsförfarande för skydd av säkerhetsskyddsklassificerade EU-uppgifter i sina egna lokaler för att garantera att det erbjuds en fysisk skyddsnivå som står i proportion till den bedömda risken. I samband med riskhanteringsprocessen ska alla relevanta faktorer beaktas, särskilt

   a) de säkerhetsskyddsklassificerade EU-uppgifternas säkerhetsskyddsklassificeringsnivå,

   b) de säkerhetsskyddsklassificerade EU-uppgifternas form och volym, med beaktande av att stora mängder eller en sammanställning av säkerhetsskyddsklassificerade EU-uppgifter kan göra det nödvändigt att tillämpa striktare skyddsåtgärder,

   c) omgivningarna kring och strukturen på byggnaderna eller området där de säkerhetsskyddsklassificerade EU-uppgifterna förvaras, och

   d) det bedömda hotet från underrättelsetjänster med unionen eller medlemsstaterna som måltavla och det hot som sabotage eller terrorism samt omstörtande eller annan brottslig verksamhet bedöms medföra.

4. Den behöriga säkerhetsmyndigheten ska med tillämpning av begreppet flernivåförsvar fastställa en lämplig kombination av fysiska säkerhetsåtgärder som ska tillämpas. Det kan röra sig om någon eller några av följande åtgärder:

   a) Inhägnad: ett fysiskt hinder som försvar för gränsen för ett skyddat område.

   b) Intrångsdetekteringssystem: ett system för att upptäcka intrång kan användas för att höja den säkerhetsnivå som ges av en inhägnad eller i rum och byggnader i stället för säkerhetspersonal eller för att bistå denna.

   c) Behörighetskontroll: kontrollen kan avse en plats, en byggnad eller byggnader på en plats eller områden eller rum i en byggnad. Den kan ske med elektroniska eller elektromekaniska metoder, med hjälp av säkerhetspersonal och/eller en receptionist, eller med någon annan fysisk metod.

   d) Säkerhetspersonal: utbildad, övervakad och när så krävs på lämpligt sätt säkerhetsprövad säkerhetspersonal kan anställas, bland annat, för att avskräcka personer som planerar dolda intrång.

   e) Övervakningskameror: övervakningskameror kan användas av säkerhetspersonalen för att kontrollera incidenter och larm från system för upptäckt av intrång på stora platser eller vid områdesgränsen.

   f) Säkerhetsbelysning: säkerhetsbelysning kan användas i avskräckande syfte mot en eventuell inkräktare och för att ge den belysning som är nödvändig för ändamålsenlig övervakning, antingen direkt med hjälp av säkerhetspersonalen eller indirekt genom ett system med övervakningskameror.

   g) Alla andra lämpliga fysiska åtgärder för att avskräcka eller upptäcka obehörigt tillträde eller för att förhindra att säkerhetsskyddsklassificerade EU-uppgifter skadas eller går förlorade.

5. Den behöriga myndigheten kan ha behörighet att i avskräckande syfte utföra kontroller vid in- eller utpassering mot otillåtet införande av material eller otillåtet bortförande av någon form av säkerhetsskyddsklassificerade EU-uppgifter från utrymmen eller byggnader.

6. När det finns en risk för att utomstående kan se säkerhetsskyddsklassificerade EU-uppgifter, även oavsiktligt, ska lämpliga åtgärder vidtas för att bemöta denna risk.

7. För nya anläggningar ska de fysiska säkerhetskraven och deras funktionsspecifikationer fastställas i samband med planeringen och utformningen av anläggningarna. För befintliga anläggningar ska de fysiska säkerhetskraven tillämpas i så stor utsträckning som möjligt.

III. UTRUSTNING FÖR FYSISKT SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

8. När den behöriga säkerhetsmyndigheten förvärvar utrustning (exempelvis säkerhetsskåp, dokumentförstörare, dörrlås, elektroniska system för kontroll av tillträde, system för upptäckt av intrång, larmsystem) för fysiskt skydd av säkerhetsskyddsklassificerade EU-uppgifter, ska den se till att utrustningen uppfyller godkända tekniska standarder och minimikrav.

9. De tekniska specifikationerna för utrustning som ska användas för det fysiska skyddet av säkerhetsskyddsklassificerade EU-uppgifter ska fastställas i säkerhetsriktlinjer som ska godkännas av säkerhetskommittén.

10. Säkerhetssystemen ska inspekteras med jämna mellanrum och utrustningen regelbundet underhållas. Vid underhållsarbetet ska inspektionsresultaten beaktas så att utrustningen fortsätter att hålla optimala prestanda.

11. De enskilda säkerhetsåtgärdernas och det övergripande säkerhetssystemets ändamålsenlighet ska vid varje inspektion bedömas på nytt.

IV. FYSISKT SKYDDADE UTRYMMEN

12. Två slag av fysiskt skyddade utrymmen, eller nationella motsvarigheter, ska skapas för att fysiskt skydda säkerhetsskyddsklassificerade EU-uppgifter, nämligen

    a) administrativa utrymmen och

    b) säkrade utrymmen (inklusive tekniskt säkrade utrymmen).

    I detta beslut ska alla hänvisningar till administrativa och säkrade områden, inklusive tekniskt säkrade områden, även anses omfatta nationella motsvarigheter.

13. Den behöriga säkerhetsmyndigheten ska fastställa att ett utrymme uppfyller kraven för att betecknas som administrativt utrymme, säkrat utrymme eller tekniskt säkrat utrymme.

14. När det gäller administrativa utrymmen

    a) ska en synlig yttre gräns upprättas som gör att personer och om möjligt fordon kan kontrolleras,

    b) ska obeledsagat tillträde endast beviljas personer som av den behöriga myndigheten vederbörligen bemyndigats att ha tillgång till dessa och

    c) övriga personer ska alltid ledsagas eller genomgå likvärdiga kontroller.

15. När det gäller säkrade utrymmen ska

    a) en synlig yttre gräns upprättas genom vilken alla in- och utpasseringar kontrolleras med hjälp av ett passerkort eller ett system för personigenkänning,

    b) obeledsagat tillträde endast beviljas personer som har säkerhetsprövats och fått särskilt tillstånd att vistas i utrymmet enligt principen om behovsenlig behörighet, och

    c) övriga personer alltid ledsagas eller genomgå likvärdiga kontroller.

16. När tillträde till ett säkrat utrymme i praktiken innebär direkt tillgång till de säkerhetsskyddsklassificerade uppgifter som finns där, ska dessutom följande krav gälla:

    a) Den högsta säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade uppgifter som normalt sett finns i området ska vara klart angiven.

    b) Alla besökare måste ha särskilt tillstånd för tillträde till området, ska alltid ledsagas och ska ha genomgått vederbörlig säkerhetsprövning, såvida åtgärder inte vidtas för att garantera att ingen tillgång till säkerhetsskyddsklassificerade EU-uppgifter är möjlig.

17. Säkrade utrymmen som skyddas mot avlyssning ska betecknas som tekniskt säkrade utrymmen. Dessutom ska följande krav gälla:

    a) Utrymmena ska vara utrustade med ett system för upptäckt av intrång, vara låsta när de är tomma och bevakas när någon vistas där. Nycklar ska kontrolleras i enlighet med avsnitt VI.

    b) Alla personer och allt material som kommer in i dessa utrymmen ska kontrolleras.

    c) Utrymmena ska vara föremål för regelbundna fysiska och/eller tekniska inspektioner enligt vad som krävs av den behöriga säkerhetsmyndigheten. Sådana inspektioner ska också genomföras efter eventuellt obehörigt intrång eller misstanke om sådant intrång.

    d) Utrymmena får inte vara utrustade med otillåtna kommunikationslinjer, otillåtna telefoner eller annan otillåten kommunikationsutrustning och elektrisk eller elektronisk utrustning.

18. Trots vad som sägs i punkt 17 d ska all slags kommunikationsutrustning och elektrisk eller elektronisk utrustning innan denna används i utrymmen där det hålls möten eller utförs arbete som omfattar uppgifter på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET och högre och där hotet mot säkerhetsskyddsklassificerade EU-uppgifter bedöms vara allvarligt, först undersökas av den behöriga säkerhetsmyndigheten som ska försäkra sig om att inga begripliga uppgifter oavsiktligt eller olagligt kan föras ut från det säkrade utrymmet genom sådan utrustning.

19. Säkrade utrymmen där tjänstgörande personal inte vistas 24 timmar om dygnet ska, när så är lämpligt, inspekteras efter den normala arbetstidens slut och med slumpvis valda mellanrum utanför normal arbetstid, utom när system för upptäckt av intrång har installerats.

20. Säkrade utrymmen och tekniskt säkrade utrymmen får tillfälligt inrättas inom ett administrativt utrymme för ett sekretessbelagt möte eller liknande ändamål.

21. Säkra driftsmetoder ska utarbetas för varje säkrat utrymme där följande fastställs:

    a) Sekretessgraden för de säkerhetsskyddsklassificerade EU-uppgifter som får hanteras och förvaras i utrymmet.

    b) Den övervakning och de skyddsåtgärder som ska upprätthållas.

    c) Vilka personer som får ges obeledsagat tillträde till utrymmet i kraft av behovsenlig behörighet och säkerhetsgodkännande.

    d) Vid behov förfaranden för ledsagare eller för skydd av säkerhetsskyddsklassificerade EU-uppgifter när besökare beviljas tillträde till utrymmet.

    e) Andra relevanta åtgärder och förfaranden.

22. Valv ska byggas inom det säkrade utrymmet. Väggarna, golven, taken, fönstren och de låsförsedda dörrarna ska godkännas av den behöriga nationella säkerhetsmyndigheten och erbjuda skydd motsvarande ett säkerhetsskåp som godkänts för förvaring av säkerhetsskyddsklassificerade EU-uppgifter med motsvarande sekretessgrad.

V. FYSISKA SKYDDSÅTGÄRDER FÖR HANTERING OCH FÖRVAR AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

23. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED får hanteras

    a) i ett säkrat utrymme,

    b) i ett administrativt utrymme, förutsatt att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från tillträde av obehöriga, eller

    c) utanför ett säkrat eller administrativt utrymme, förutsatt att innehavaren befordrar de säkerhetsskyddsklassificerade EU-uppgifterna i enlighet med punkterna 28–41 i bilaga III och har åtagit sig att följa de kompensationsåtgärder som anges i säkerhetsföreskrifterna från den behöriga myndigheten för att garantera att säkerhetsskyddsklassificerade EU-uppgifter skyddas från tillträde av obehöriga.

24. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED ska förvaras i lämpliga låsbara kontorsmöbler i ett administrativt eller säkrat utrymme. De får tillfälligt lagras utanför ett säkrat eller administrativt utrymme, förutsatt att innehavaren har åtagit sig att följa de kompensationsåtgärder som anges i säkerhetsanvisningarna från den behöriga myndigheten.

25. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET får hanteras

    a) i ett säkrat utrymme,

    b) i ett administrativt utrymme, förutsatt att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från tillträde av obehöriga, eller

    c) utanför ett säkrat eller administrativt utrymme förutsatt att innehavaren

        i) befordrar de säkerhetsskyddsklassificerade EU-uppgifterna i enlighet med punkterna 28–41 i bilaga III,

        ii) har åtagit sig att följa de kompensationsåtgärder som anges i säkerhetsanvisningarna från den behöriga myndigheten, för att garantera att säkerhetsskyddsklassificerade EU-uppgifter skyddas från tillträde av obehöriga,

        iii) alltid har de säkerhetsskyddsklassificerade EU-uppgifterna under sin personliga kontroll, och

        iv) om dokumenten är i pappersform, har meddelat det behöriga registret detta.

26. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska förvaras i ett säkrat utrymme i antingen ett säkerhetsskåp eller ett valv.

27. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET ska hanteras i ett säkrat utrymme.

28. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET ska förvaras i ett säkrat utrymme under något av följande förhållanden:

    a) I ett säkerhetsskåp, i överensstämmelse med punkt 8, med minst en av följande kompletterande kontroller:

        i) Kontinuerligt skydd eller kontroll av säkerhetsprövad personal eller vakthavande personal.

        ii) Ett godkänt system för upptäckt av intrång i kombination med insatspersonal för säkerheten.

    b) I ett valv utrustat med system för upptäckt av intrång i kombination med säkerhetspersonal redo att ingripa om det skulle behövas.

29. Bestämmelserna om befordran av säkerhetsskyddsklassificerade EU-uppgifter utanför fysiskt säkrade utrymmen anges i bilaga III.

VI. KONTROLL AV NYCKLAR OCH KOMBINATIONER SOM ANVÄNDS FÖR ATT SKYDDA SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

30. Den behöriga säkerhetsmyndigheten ska fastställa förfaranden för hantering av nycklar och kombinationer för kontor, rum, valv och säkerhetsskåp. Dessa förfaranden ska skydda mot obehörig tillgång.

31. Kombinationer ska memoreras av lägsta möjliga antal personer som behöver känna till dem. Kombinationer för säkerhetsskåp och valv avsedda för förvaring av säkerhetsskyddsklassificerade EU-uppgifter ska ändras

    a) vid mottagande av ett nytt säkerhetsskåp,

    b) vid varje byte av personal som känner till kombinationen,

    c) vid röjande eller vid misstanke om detta,

    d) när ett lås har genomgått underhållsarbete eller reparation, och

    e) minst var tolfte månad.

BILAGA III

HANTERING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 9. I bilagan fastställs administrativa åtgärder för att kontrollera säkerhetsskyddsklassificerade EU-uppgifter genom deras hela livscykel för att avskräcka och upptäcka avsiktligt eller oavsiktligt röjande eller förlust av dessa uppgifter.

II. REGLER FÖR SÄKERHETSSKYDDSKLASSIFICERINGEN

Säkerhetsskyddsklassificeringsnivåer och säkerhetsskyddsmarkeringar

2. Uppgifter ska säkerhetsskyddsklassificeras när deras konfidentialitet behöver skyddas.

3. Den som är upphovsman till säkerhetsskyddsklassificerade EU-uppgifter ska vara ansvarig för fastställandet av uppgifternas säkerhetsskyddsklassificeringsnivå i enlighet med de relevanta riktlinjerna för säkerhetsskyddsklassificering och för den första spridningen av uppgifterna.

4. Säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter ska fastställas i enlighet med artikel 2.2 och genom hänvisning till den säkerhetsstrategi som ska godkännas av rådet i enlighet med artikel 3.3.

5. Säkerhetsskyddsklassificeringsnivån ska anges klart och korrekt, oberoende av huruvida de säkerhetsskyddsklassificerade EU-uppgifterna är i pappersform, muntlig, elektronisk eller någon annan form.

6. Enstaka delar av en viss handling (dvs. sidor, stycken, avsnitt, bilagor, tillägg och annat bifogat material) kan kräva inplacering på en annan säkerhetsskyddsklassificeringsnivå och ska markeras i enlighet med detta, även när de förvaras i elektronisk form.

7. Den övergripande säkerhetsskyddsklassificeringsnivån för en handling eller en datafil ska vara minst lika hög som den del som fått den högsta säkerhetsskyddsklassificeringsnivån. När uppgifter från olika källor sammanställs, ska den slutliga produkten ses över för att dess övergripande säkerhetsskyddsklassificeringsnivå ska kunna fastställas, eftersom den kan motivera en högre säkerhetsskyddsklassificeringsnivå än säkerhetsskyddsklassificeringsnivån för de enskilda delarna.

8. I största möjliga utsträckning ska handlingar som innehåller delar på olika säkerhetsskyddsklassificeringsnivåer struktureras så att delar på olika säkerhetsskyddsklassificeringsnivå vid behov lätt kan identifieras och avskiljas.

9. Ett brev eller en not som åtföljs av bifogade handlingar ska ha samma säkerhetsskyddsklassificeringsnivå som den högsta säkerhetsskyddsklassificeringsnivån hos bilagorna. Upphovsmannen ska tydligt ange på vilken nivå de ska säkerhetsskyddsklassificeras när de skilts från de bifogade handlingarna med hjälp av en lämplig markering, t.ex. följande:

CONFIDENTIEL UE/EU CONFIDENTIAL

Utan bilaga/bilagor RESTREINT UE/EU RESTRICTED

Markeringar

10. Utöver de säkerhetsskyddsklassificeringsnivåer som anges i artikel 2.2 får säkerhetsskyddsklassificerade EU-uppgifter förses med ytterligare markeringar, till exempel följande:

a) En markering som anger upphovsman.

b) Delgivningsbegränsning, kodord eller akronymer som anger vilket verksamhetsområde som handlingen rör, särskild spridning grundad på principen om behovsenlig behörighet eller begränsad användning.

c) Markering om att uppgifter får lämnas ut, eller

d) i förekommande fall datum eller särskild händelse efter vilken uppgifterna får inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerade.

Förkortade säkerhetsskyddsmarkeringar

11. Standardiserade förkortade säkerhetsskyddsmarkeringar får användas för att ange säkerhetsskyddsklassificeringsnivån för enskilda stycken i en text. Förkortade säkerhetsskyddsmarkeringar får inte ersätta de fullständiga säkerhetsskyddsmarkeringarna.

12. Följande standardförkortningar får användas i säkerhetsskyddsklassificerade EU-handlingar för att ange säkerhetsskyddsklassificeringsnivån för avsnitt eller textstycken vars storlek är mindre än en sida:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Upprättande av säkerhetsskyddsklassificerade EU-handlingar

13. När en säkerhetsskyddsklassificerad EU-handling upprättas ska

a) varje sida tydligt märkas med säkerhetsskyddsklassificeringsnivån,

b) varje sida numreras,

c) handlingen förses med ett referensnummer och en ämnesuppgift som inte i sig är en säkerhetsskyddsklassificerad uppgift, om den inte getts en sådan märkning,

d) handlingen dateras, och

e) handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller högre ha ett exemplarnummer på varje sida, om de sänds ut i flera exemplar.

14. Om det inte är möjligt att tillämpa punkt 13 på de säkerhetsskyddsklassificerade EU-uppgifterna ska andra lämpliga åtgärder vidtas i enlighet med säkerhetsriktlinjer som ska fastställas i enlighet med artikel 6.2.

Inplacering på lägre säkerhetsskyddsklassificeringsnivå och beslut om att uppgifter inte längre ska vara säkerhetsskyddsklassificerade

15. När uppgifterna skapas ska upphovsmannen om möjligt, särskilt när det gäller uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, ange huruvida de säkerhetsskyddsklassificerade EU-uppgifterna kan inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade kan meddelas vid en viss tidpunkt eller efter en särskild händelse.

16. Generalsekretariatet och medlemsstaterna ska regelbundet se över säkerhetsskyddsklassificerade EU-uppgifter för att förvissa sig om att säkerhetsskyddsklassificeringsnivån fortfarande gäller. Generalsekretariatet ska inrätta ett system för att säkerställa att säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som det har givit upphov till ses över minst vart femte år. En sådan översyn är inte nödvändig om upphovsmannen redan från början har angett att uppgifterna automatiskt kommer att inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller att beslut om att uppgifterna inte längre behöver vara säkerhetsskyddsklassificerade kommer att meddelas och uppgifterna har märkts i enlighet med detta.

III. REGISTRERING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER FÖR SÄKERHETSÄNDAMÅL

17. För varje organisatorisk enhet inom generalsekretariatet och medlemsstaternas nationella förvaltningar där säkerhetsskyddsklassificerade EU-uppgifter hanteras ska det fastställas en ansvarig registreringsenhet i syfte att säkerställa att uppgifterna hanteras i enlighet med detta beslut. Registreringsenheterna ska inrättas som säkrade utrymmen enligt definitionen i bilaga II.

18. I detta beslut avses med registrering för säkerhetsändamål (nedan kallat *registrering*) tillämpning av förfaranden som registrerar materialets livscykel, inbegripet dess spridning och förstöring.

19. Allt material på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre ska registreras i de därför avsedda registren när de anländer till eller lämnar en organisatorisk enhet.

20. Den centrala registreringsenheten vid generalsekretariatet ska föra ett register över alla säkerhetsskyddsklassificerade uppgifter som lämnas ut av rådet och generalsekretariatet till tredjestater och internationella organisationer, och över alla säkerhetsskyddsklassificerade uppgifter som tas emot från tredjestater eller internationella organisationer.

21. När det gäller ett kommunikations- och informationssystem, får förfarandena utföras genom processer i själva kommunikations- och informationssystemet.

22. Rådet ska godkänna en säkerhetsstrategi för registrering av säkerhetsskyddsklassificerade EU-uppgifter för säkerhetsändamål.

Register för handlingar med beteckningen TRÈS SECRET UE/EU TOP SECRET

23. En registreringsenhet ska utses i medlemsstaterna och generalsekretariatet för att fungera som central myndighet för mottagning och avsändning av uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET. Om det är nödvändigt får underenheter utses för att hantera sådana uppgifter för registreringsändamål.

24. Sådana underenheter får inte överföra handlingar på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET direkt till andra underenheter som är underställda samma centrala registreringsenhet för TRÈS SECRET UE/EU TOP SECRET eller externt utan uttryckligt godkännande från det senare.

IV. KOPIERING OCH ÖVERSÄTTNING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-HANDLINGAR

25. Handlingar på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET får inte kopieras eller översättas utan föregående skriftligt medgivande från upphovsmannen.

26. Om upphovsmannen till handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET och lägre inte har angett begränsning för kopiering eller översättning, får sådana handlingar kopieras eller översättas på uppdrag av innehavaren.

27. De säkerhetsåtgärder som ska tillämpas på originaldokumentet ska även tillämpas på kopior och översättningar av detta.

V. BEFORDRAN AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

28. Befordran av säkerhetsskyddsklassificerade EU-uppgifter ska omfattas av skyddsåtgärderna i punkterna 30–41. När säkerhetsskyddsklassificerade EU-uppgifter befordras via elektroniska medier, och trots vad som sägs i artikel 9.4, får skyddsåtgärderna nedan kompletteras med lämpliga tekniska motåtgärder som föreskrivs av den behöriga säkerhetsmyndigheten för att minimera risken för att uppgifterna går förlorade eller röjs.

29. De behöriga säkerhetsmyndigheterna i generalsekretariatet och i medlemsstaterna ska utfärda anvisningar för befordran av säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut.

Inom en byggnad eller ett autonomt byggnadskomplex

30. Säkerhetsskyddsklassificerade EU-uppgifter som befordras inom en byggnad eller ett autonomt byggnadskomplex ska vara övertäckta så att det inte går att se innehållet.

31. Inom en byggnad eller ett autonomt byggnadskomplex ska uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET befordras i ett förseglat kuvert försett med enbart adressatens namn.

Inom unionen

32. Säkerhetsskyddsklassificerade EU-uppgifter som befordras mellan byggnader eller lokaler inom unionen ska förpackas så att de skyddas från obehörigt röjande.

33. Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET inom unionen ska ske på något av följande sätt:

a) Genom militär-, regerings- eller diplomatkurir, när så är lämpligt.

b) Genom personligt överlämnande, förutsatt att

i) de säkerhetsskyddsklassificerade EU-uppgifterna inte lämnas utan uppsikt av budet, såvida de inte förvaras i enlighet med bestämmelserna i bilaga II,

ii) de säkerhetsskyddsklassificerade EU-uppgifterna inte öppnas under befordran eller läses på offentlig plats,

iii) budet blir upplyst om sina säkerhetsskyldigheter, och

iv) budet förses med ett kuririntyg när så krävs.

c) Genom posttjänster eller kommersiella kurirtjänster under förutsättning att

i) de är godkända av de relevanta nationella säkerhetsmyndigheterna enligt nationella lagar och andra författningar, och

ii) de tillämpar lämpliga skyddsåtgärder enligt de minimikrav som ska fastställas i säkerhetsriktlinjer enligt artikel 6.2.

Vid befordran från en medlemsstat till en annan ska bestämmelserna i led c begränsas till att gälla uppgifter upp till säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED får också befordras med nationella posttjänster eller kommersiella kurirtjänster. Kuririntyg krävs inte för befordran av sådana uppgifter.

35. Material på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET (t.ex. utrustning eller maskiner) som inte kan befordras på det sätt som avses i punkt 33 ska transporteras såsom frakt av kommersiella transportörer i enlighet med bilaga V.

36. Fysisk befordran av uppgifter på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET eller högre mellan byggnader eller lokaler inom unionen ska ske med militär-, regerings- eller diplomatkurir, när så är lämpligt.

Från unionen till en tredjestat

37. Säkerhetsskyddsklassificerade EU-uppgifter som befordras från unionen till en tredjestat ska förpackas så att de skyddas från obehörigt röjande.

38. Fysisk befordran av uppgifter på en säkerhetsskyddsklassificeringsnivå upp till SECRET UE/EU SECRET från unionen till en tredjestat ska ske på något av följande sätt:

a) Genom militär- eller diplomatkurir.

b) Genom personligt överlämnande förutsatt att

i) paketet är försett med ett officiellt sigill eller är förpackat på ett sådant sätt att det framgår att det rör sig om en officiell försändelse som inte bör genomgå tull- eller säkerhetskontroll,

ii) buden bär med sig ett kuririntyg som fastställer paketets identitet och ger dem behörighet att befordra paketet,

iii) säkerhetsskyddsklassificerade EU-uppgifter inte lämnas utan uppsikt av budet, såvida de inte förvaras i enlighet med bestämmelserna i bilaga II,

iv) säkerhetsskyddsklassificerade EU-uppgifter inte öppnas under befordran eller läses på offentlig plats, och

v) budet blir upplyst om sina säkerhetsskyldigheter.

39. Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som unionen lämnat till en tredjestat eller internationell organisation ska uppfylla de relevanta bestämmelserna i ett informationssäkerhetsavtal eller en administrativ överenskommelse enligt artikel 13.2 a eller b.

40. Uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED får också befordras med nationella posttjänster eller kommersiella kurirtjänster.

41. Befordran av information på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET från unionen till en tredjestats territorium ska ske med militär- eller diplomatkurir.

VI. FÖRSTÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

42. Säkerhetsskyddsklassificerade EU-uppgifter som inte längre behövs får destrueras, utan att det påverkar relevanta bestämmelser om arkivering.

43. Handlingar som är föremål för registrering i enlighet med artikel 9.2 ska destrueras av den ansvariga registreringsenheten enligt innehavarens eller en behörig myndighets anvisningar. Diarier och andra registreringsuppgifter ska uppdateras i enlighet med detta.

44. För handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller TRÈS SECRET UE/EU TOP SECRET ska förstöringen utföras i närvaro av ett vittne som har säkerhetsgodkänts för minst den säkerhetsskyddsklassificeringsnivå som anges på handlingen som ska destrueras.

45. Registratorn och vittnet om den senares närvaro krävs, ska underteckna ett förstöringsintyg som ska arkiveras vid registreringsenheten. Registreringsenheten ska bevara förstöringsintyg för handlingar på säkerhetsskyddsklassificeringsnivån TRÈS SECRET UE/EU TOP SECRET i minst tio år och för handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET i minst fem år.

46. Säkerhetsskyddsklassificerade handlingar, inklusive sådana på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, ska destrueras enligt metoder som uppfyller relevant unionsstandard eller likvärdiga standarder eller som har godkänts av medlemsstaterna i enlighet med nationella tekniska standarder för att hindra hel eller partiell rekonstruktion.

47. Förstöring av lagringsmedier för datorer som använts för säkerhetsskyddsklassificerade EU-uppgifter ska ske i enlighet med punkt 37 i bilaga IV.

48. I nödsituationer ska säkerhetsskyddsklassificerade EU-uppgifter, om det föreligger omedelbar risk för obehörigt röjande, förstöras av innehavaren på ett sådant sätt att de varken helt eller delvis kan rekonstrueras. Upphovsmannen och den registreringsenhet som uppgifterna härrör från ska informeras om att de registrerade säkerhetsskyddsklassificerade EU-uppgifterna på grund av nödsituationen har förstörts.

VII. UTVÄRDERINGSBESÖK

49. Termen utvärderingsbesök ska nedan användas för att beteckna alla

a) inspektioner eller utvärderingsbesök i enlighet med artiklarna 9.3 och 16.2 e, f och g, eller

b) utvärderingsbesök i enlighet med artikel 13.5,

för bedömning av effektiviteten i de åtgärder som genomförs för att skydda säkerhetsskyddsklassificerade EU-uppgifter.

50. Utvärderingsbesök ska bland annat genomföras för att

a) säkerställa att de minimisäkerhetsnormer för skydd av säkerhetsskyddsklassificerade EU-uppgifter som fastställs i detta direktiv respekteras,

b) betona vikten av säkerhet och en effektiv riskhantering inom de inspekterade enheterna,

c) rekommendera motåtgärder för att minska de specifika konsekvenserna av att de säkerhetsskyddsklassificerade uppgifternas konfidentialitet, riktighet eller tillgänglighet går förlorad och

d) förstärka säkerhetsmyndigheternas fortlöpande program för utbildning och medvetandegörande när det gäller säkerhet.

51. Rådet ska före utgången av varje kalenderår anta det program för utvärderingsbesök som föreskrivs i artikel 16.1 c för det påföljande året. De faktiska tidpunkterna för varje utvärderingsbesök ska fastställas i samförstånd med den unionsbyrå eller det unionsorgan, den medlemsstat, tredjestat eller internationella organisation som berörs.

Genomförande av utvärderingsbesök

52. Utvärderingsbesök ska genomföras för att kontrollera relevanta föreskrifter och förfaranden vid den besökta enheten och verifiera att dess praxis uppfyller de grundläggande principer och miniminormer som fastställs i detta beslut och i de bestämmelser som reglerar utbytet av säkerhetsskyddsklassificerade uppgifter med den enheten.

53. Utvärderingsbesöken ska genomföras i två etapper. Före själva besöket ska vid behov ett förberedande möte anordnas med den berörda enheten. Efter detta förberedande möte ska utvärderingsgruppen i samförstånd med den nämnda enheten göra upp ett detaljerat program för utvärderingsbesöket omfattande samtliga säkerhetsområden. Utvärderingsgruppen bör ha tillträde till alla platser där säkerhetsskyddsklassificerade EU-uppgifter hanteras, särskilt registreringsenheter samt kommunikations- och informationssystemets anslutningspunkter (”points of presence”).

54. Utvärderingsbesök vid medlemsstaternas nationella myndigheter, tredjestater och internationella organisationer ska genomföras i fullständigt samarbete med den besökta enhetens, tredjestatens eller internationella organisationens tjänstemän.

55. Utvärderingsbesök vid unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer ska genomföras med bistånd av experter från den nationella säkerhetsmyndighet på vars territorium organet eller byrån ligger.

56. Vid utvärderingsbesök vid unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer och i tredjestater och internationella organisationer får hjälp av experter från de nationella säkerhetsmyndigheterna begäras i enlighet med närmare förfaranden som ska godkännas av säkerhetskommittén.

Rapporter

57. Efter avslutat utvärderingsbesök ska de viktigaste slutsatserna och rekommendationerna presenteras för den besökta enheten. Därefter ska en rapport om utvärderingsbesöket utarbetas. Om korrigerande åtgärder och rekommendationer har föreslagits, ska tillräckligt detaljerade uppgifter för att underbygga de slutsatser som nåtts ingå i rapporten. Rapporten ska sändas till den behöriga myndigheten för den besökta enheten.

58. För utvärderingsbesök som genomförs i medlemsstaternas nationella förvaltningar ska följande gälla:

a) Utkastet till utvärderingsrapport ska översändas till den berörda nationella säkerhetsmyndigheten så att det kan kontrolleras att fakta stämmer och att inga uppgifter på högre säkerhetsskyddsklassificeringsnivå än RESTREINT UE/EU RESTRICTED ingår i rapporten.

b) Såvida inte den berörda medlemsstatens nationella säkerhetsmyndighet begär att utvärderingsrapporterna inte ska spridas, ska de tillställas säkerhetskommittén. Rapporten ska placeras på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

En återkommande rapport ska utarbetas under ansvar av säkerhetsmyndigheten vid generalsekretariatet (säkerhetsavdelningen) med fokus på de viktigaste frågorna samt de viktigaste erfarenheterna från de utvärderingsbesök som genomförts i medlemsstaterna under en specificerad tidsperiod och ska granskas av säkerhetskommittén.

59. För utvärderingsbesök i tredjestater och vid internationella organisationer ska rapporten översändas till säkerhetskommittén. Rapporten ska minst placeras på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED. Alla korrigerande åtgärder ska kontrolleras under ett uppföljningsbesök och rapporteras till säkerhetskommittén.

60. För utvärderingsbesök vid unionens organ, byråer och enheter som tillämpar detta beslut eller dess principer ska rapporterna om utvärderingsbesöken översändas till säkerhetskommittén. Utkastet till rapport om utvärderingsbesöket ska översändas till den berörda byrån eller det berörda organet, så att det kan kontrolleras att fakta stämmer och att inga uppgifter på högre säkerhetsskyddsklassificeringsnivå än RESTREINT UE/EU RESTRICTED ingår i rapporten. Alla korrigerande åtgärder ska kontrolleras under ett uppföljningsbesök och rapporteras till säkerhetskommittén.

61. Säkerhetsmyndigheten vid generalsekretariatet ska genomföra regelbundna inspektioner av organisatoriska enheter inom generalsekretariatet för de ändamål som fastställs i punkt 50.

Checklista

62. Säkerhetsmyndigheten vid generalsekretariatet ska utarbeta och uppdatera en checklista för de punkter som ska kontrolleras under ett utvärderingsbesök. Denna checklista ska översändas till säkerhetskommittén.

63. Nödvändiga uppgifter för att fylla i checklistan ska framför allt inhämtas under besöket från säkerhetsledningen vid den enhet som inspekteras. När checklistan har fyllts i med detaljerade svar, ska den klassificeras i samförstånd med den inspekterade enheten. Den ska inte utgöra en del av inspektionsrapporten.

BILAGA IV

SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER SOM HANTERAS I KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 10.

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

Autenticitet: Garanti för att uppgifterna är riktiga och härrör från angivna källor.

Tillgänglighet: Egenskapen att finnas tillgänglig och vara användbar för en behörig enhet.

Konfidentialitet: Egenskapen att uppgifter skyddas mot insyn av obehöriga personer, enheter eller processer.

Riktighet: Egenskapen att skydda att uppgifter och tillgångar är exakta och fullständiga.

Oavvislighet: Möjlighet att bevisa att en åtgärd eller händelse har ägt rum så att denna händelse eller åtgärd inte senare kan förnekas.

II. PRINCIPER FÖR INFORMATIONSSÄKRING

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

Hantering av säkerhetsrisker

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

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

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

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

Säkerhet under kommunikations- och informationssystemets hela livscykel

8. Att garantera säkerheten ska vara ett krav under systemets hela livscykel, från inledandet till avvecklingen av systemet.

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

10. Varje system, inbegripet tekniska och icke-tekniska säkerhetsåtgärder, ska säkerhetstestas under godkännandeprocessen för att säkerställa att rätt säkerhetsnivå erhålls och för att kontrollera att de är korrekt genomförda, integrerade och konfigurerade.

11. Säkerhetsutvärderingar, inspektioner och översyner ska regelbundet genomföras under ett systems drift och underhåll och när exceptionella omständigheter uppkommer.

12. Systemets säkerhetsdokumentering ska utvecklas under dess livscykel såsom en integrerad del av processen för hantering av ändringar och konfiguration.

Bästa praxis

13. Generalsekretariatet och medlemsstaterna ska samarbeta för att ta fram bästa praxis för skydd av säkerhetsskyddsklassificerade EU-uppgifter som behandlas i systemet. Riktlinjer för bästa praxis ska ange tekniska, fysiska, organisatoriska och procedurmässiga säkerhetsåtgärder för system vilkas ändamålsenlighet för att motverka givna hot och sårbarheter har bevisats.

14. Vid skyddet av säkerhetsskyddsklassificerade EU-uppgifter som behandlas i systemet ska man utnyttja erfarenheterna vid de enheter som deltar i informationssäkring, både inom och utanför unionen.

15. Spridningen och det efterföljande genomförandet av bästa praxis ska bidra till uppnåendet av en likvärdig säkerhetsnivå för de olika system som används av generalsekretariatet och medlemsstaterna i vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras.

Flernivåförsvar

16. För att minska risken för kommunikations- och informationssystem ska en rad tekniska och icke-tekniska säkerhetsåtgärder genomföras, organiserade som flera försvarsnivåer. Dessa nivåer ska omfatta följande:

a) *Avskräckning:* Säkerhetsåtgärder vars syfte är att avstyra eventuella planer på att angripa systemet.

b) *Förhindrande:* Säkerhetsåtgärder vars syfte är att hindra eller blockera ett angrepp mot systemet.

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

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

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

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

17. Den nationella säkerhetsmyndigheten eller en annan behörig myndighet ska se till att

a) kapacitet för it-försvar inrättas så att hot som kan gå utöver organisatoriska och nationella gränser kan bemötas och

b) motåtgärder samordnas och information utbyts om dessa hot, incidenter och risker (kapacitet för incidenthantering).

Principen om minimalitet och begränsad behörighet

18. Endast väsentliga funktioner, apparater och tjänster för att uppfylla driftskraven ska utnyttjas för att undvika onödiga risker.

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

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

Medvetenhet om informationssäkring

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

a) att säkerhetshaverier kan förorsaka betydande skada i systemet,

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

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

22. För att säkerställa denna insikt om ansvaret för säkerheten ska utbildning i informationssäkring och medvetenhet vara obligatorisk för all inblandad personal, inbegripet den högre ledningen och systemanvändare.

Utvärdering och godkännande av produkter för it-säkerhet

23. Den grad av förtroende som krävs i säkerhetsåtgärderna, definierad som en säkerhetsnivå, ska fastställas i enlighet med resultaten av riskhanteringsprocessen och i linje med relevanta säkerhetsstrategier och säkerhetsriktlinjer.

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

25. Kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter ska evalueras och godkännas av en medlemsstats nationella kryptogodkännande myndighet.

26. Innan sådana kryptoprodukter rekommenderas för godkännande av rådet eller generalsekreteraren i enlighet med artikel 10.6 ska de ha genomgått och klarat en andrapartsevaluering av en medlemsstats kvalificerade utvärderingsmyndighet (AQUA) som inte har deltagit i utformningen eller tillverkningen av utrustningen. Hur detaljerad andrapartsevalueringen ska vara beror på den planerade högsta säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som ska skyddas genom dessa produkter. Rådet ska godkänna en säkerhetsstrategi för utvärdering och godkännande av kryptoprodukter.

27. När det är motiverat av särskilda operativa skäl får i förekommande fall rådet eller generalsekreteraren på rekommendation av säkerhetskommittén medge undantag från kraven i punkt 25 eller 26 i denna bilaga och bevilja interimsgodkännande för en viss period i enlighet med förfarandet i artikel 10.6.

28. Rådet får, på rekommendation av säkerhetskommittén, godta en tredjestats eller en internationell organisations metod för utvärdering, urval och godkännande av kryptoprodukter och i enlighet med detta godkänna sådana kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter som lämnas ut till tredjestaten eller den internationella organisationen i fråga.

29. En kvalificerad utvärderingsmyndighet (AQUA) ska vara en kryptogodkännande myndighet i en medlemsstat, vilken har ackrediterats på grundval av kriterier som rådet har fastställt för att genomföra andrapartsevalueringen av kryptoprodukter för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

30. Rådet ska godkänna en säkerhetsstrategi för kvalificering och godkännande av sådana produkter för it-säkerhet som inte används för kryptering.

Överföring inom säkrade och administrativa områden

31. När överföringen av säkerhetsskyddsklassificerade EU-uppgifter är begränsad till säkrade områden eller administrativa utrymmen, får trots bestämmelserna i detta beslut okrypterad överföring eller kryptering på en lägre nivå användas på grundval av resultatet av riskhanteringsförfarandet och med godkännande från ackrediteringsmyndigheten för säkerhet.

Säker sammankoppling mellan kommunikations- och informationssystemen

32. I detta direktiv avses med sammankoppling en direkt förbindelse mellan två eller flera it-system i syfte att utbyta uppgifter och andra informationstillgångar (t.ex. kommunikation) i form av envägs- eller flervägskommunikation.

33. Alla it-system som sammankopplats ska inledningsvis behandlas som icke-tillförlitliga och skyddsåtgärder ska införas för att kontrollera utbytet av säkerhetsskyddsklassificerade uppgifter.

34. För all sammankoppling av system för säkerhetsskyddsklassificerade EU-uppgifter med ett annat it-system ska följande grundläggande krav uppfyllas:

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

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

c) Gränsskyddstjänster ska genomföras vid den yttre säkerhetsgränsen för samtliga system.

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

    När det oskyddade eller allmänna nätet används enbart som nätoperatör och data är krypterade med en kryptoprodukt som godkänts i enlighet med artikel 10 ska en sådan sammankoppling inte betraktas som samtrafik.

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

Lagringsmedier för datorer

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

38. Lagringsmedier för datorer ska återanvändas, inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade i enlighet med säkerhetsriktlinjer som ska fastställas enligt artikel 6.2.

Nödlägen

39. Trots bestämmelserna i detta beslut får de särskilda förfaranden som beskrivs nedan tillämpas i en nödsituation, exempelvis under en överhängande eller faktisk kris, konflikt, eller krigssituationer eller under exceptionella operativa omständigheter.

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

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

    b) det säkerhetsskyddsklassificerade materialet inte kan befordras i tid på något annat sätt.

41. Säkerhetsskyddsklassificerade EU-uppgifter som överförs under de omständigheter som anges i punkt 39 får inte vara försedda med någon märkning eller några tecken som skiljer dem från ett meddelande som inte är sekretessbelagt eller som kan skyddas genom någon tillgänglig kryptoprodukt. Mottagarna ska utan dröjsmål underrättas om säkerhetsskyddsklassificeringsnivån på annat sätt.

42. Om punkt 39 tillämpas, ska därefter en rapport lämnas till den behöriga myndigheten och till säkerhetskommittén.

III. FUNKTIONER OCH MYNDIGHETER FÖR INFORMATIONSSÄKRING

43. Följande funktioner för informationssäkring ska fastställas i medlemsstaterna och vid generalsekretariatet. Dessa funktioner förutsätter inte att det finns enskilda organisatoriska enheter. De ska ha olika mandat. Emellertid får dessa funktioner, och deras medföljande ansvarsområden, kombineras eller integreras i samma organisatoriska enhet eller delas upp i olika organisatoriska enheter, förutsatt att interna intresse- eller uppdragskonflikter undviks.

Myndigheten för informationssäkring

44. Myndigheten för informationssäkring ska ansvara för att

    a) utveckla strategier och säkerhetsriktlinjer för informationssäkring och övervaka hur ändamålsenliga och relevanta dessa är,

    b) skydda och administrera teknisk information som rör kryptoprodukter,

    c) se till att de åtgärder för informationssäkring som väljs för skydd av säkerhetsskyddsklassificerade EU-uppgifter överensstämmer med relevant policy för deras lämplighet och urval,

    d) se till att kryptoprodukter väljs ut i överensstämmelse med policyn för deras lämplighet och urval,

    e) samordna utbildning i och medvetenhet om informationssäkring,

    f) samråda med systemleverantören, säkerhetsaktörerna och företrädarna för användare när det gäller säkerhetsstrategier och säkerhetsriktlinjer för informationssäkring, och

    g) se till att det finns tillgång till lämplig sakkunskap vid säkerhetskommitténs expertundergrupp för informationssäkringsfrågor.

Tempestmyndigheten

45. Tempestmyndigheten ska ansvara för att kommunikations- och informationssystemet överensstämmer med tempeststrategier och -riktlinjer. Den ska godkänna tempestmotåtgärder för anläggningar och produkter för att i driftsmiljön skydda säkerhetsskyddsklassificerade EU-uppgifter upp till en fastställd säkerhetsskyddsklassificeringsnivå.

Den kryptogodkännande myndigheten

46. Den kryptogodkännande myndigheten ska ansvara för att kryptoprodukter överensstämmer med nationell kryptopolicy eller rådets kryptopolicy. Den ska bevilja godkännande av en kryptoprodukt för att skydda säkerhetsskyddsklassificerade EU-uppgifter i deras driftsmiljö upp till en fastställd säkerhetsskyddsklassificeringsnivå. När det gäller medlemsstaterna ska den kryptogodkännande myndigheten dessutom ansvara för utvärderingen av kryptoprodukter.

Kryptodistributionsmyndigheten

47. Kryptodistributionsmyndigheten ska ansvara för att

a) förvalta och redovisa EU-krypterat material,

b) säkerställa att lämpliga förfaranden följs och att kanaler upprättas för redovisning, säker hantering, förvaring och distribution av allt EU-krypterat material, och

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

Ackrediteringsmyndigheten för säkerhet

48. Ackrediteringsmyndigheten för säkerhet för varje system ska ansvara för att

a) garantera att kommunikations- och informationssystemen överensstämmer med relevanta säkerhetsstrategier och säkerhetsriktlinjer, tillhandahålla ett intyg om godkännande av systemen för att i driftsmiljön skydda säkerhetsskyddsklassificerade EU-uppgifter upp till en fastställd säkerhetsskyddsklassificeringsnivå, i vilket man anger villkoren för säkerhetsgodkännandet och de kriterier enligt vilka nytt godkännande kommer att krävas,

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

c) fastställa en säkerhetsackrediteringsstrategi med angivande av vilken detaljgrad för ackreditering som motsvarar den säkerhetsnivå som krävs,

d) granska och godkänna säkerhetsrelaterad dokumentation, inbegripet riskhantering och redovisning av kvarstående risker, systemspecifika säkerhetskrav, kontrolldokumentering av genomförandet av säkerhet och säkra driftsmetoder samt säkerställa att detta överensstämmer med rådets säkerhetsbestämmelser och säkerhetsstrategier,

e) kontrollera genomförandet av säkerhetsåtgärder avseende systemen genom att själv genomföra eller stödja säkerhetsutvärderingar, inspektioner och översyner,

f) fastställa säkerhetskrav (t.ex. nivåer för personalgodkännande) för känsliga befattningar inom systemet,

g) stödja urval av godkända kryptoprodukter och tempestprodukter som används för säkra ett kommunikations- och informationssystem,

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

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

49. Ackrediteringsmyndigheten för säkerhet vid generalsekretariatet ska ansvara för att ackreditera alla kommunikations- och informationssystem som är i drift enligt uppdraget från generalsekretariatet.

50. Den relevanta ackrediteringsmyndigheten för säkerhet i en medlemsstat ska ansvara för att ackreditera kommunikations- och informationssystem och systemkomponenter som är i drift enligt uppdraget från medlemsstaten.

51. En gemensam ackrediteringsnämnd för säkerhet ska ansvara för ackreditering av system som omfattas av uppdraget från såväl generalsekretariatets som medlemsstaternas ackrediteringsmyndigheter för säkerhet. Den ska bestå av en företrädare för ackrediteringsmyndigheten för säkerhet från varje medlemsstat, och en företrädare för kommissionens ackrediteringsmyndighet för säkerhet ska vara närvarande vid dess möten. Andra enheter med noder i ett kommunikations- och informationssystem ska bjudas in till de möten där det systemet tas upp till diskussion.

Nämndens ordförande ska vara en företrädare för generalsekretariatets ackrediteringsmyndighet för säkerhet. Nämnden ska besluta med konsensus mellan företrädare för institutionernas ackrediteringsmyndigheter för säkerhet, medlemsstaterna och andra enheter med noder i kommunikations- och informationssystemet. Den ska periodiskt avlägga rapport om sin verksamhet till säkerhetskommittén och underrätta denna om alla redovisningar av ackreditering.

Den driftsansvariga myndigheten för informationssäkring

52. Den driftsansvariga myndigheten för informationssäkring för varje system ska ansvara för att

a) utveckla säkerhetsdokumentation i linje med säkerhetsstrategier och säkerhetsriktlinjer, särskilt systemspecifika säkerhetskrav, inbegripet redovisning av kvarstående risker, säkra driftsmetoder och kryptoplanen inom godkännandeprocessen för kommunikations- och informationssystemet,

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

c) delta i urvalet av säkerhetsåtgärder och säkerhetsutrustning avseende Tempest om det finns systemspecifika säkerhetskrav och se till att dessa installeras på ett säkert sätt och underhålls i samarbete med tempestmyndigheten,

d) övervaka genomförande och tillämpning av säkra driftsmetoder och vid behov delegera säkerhetsansvaret för driften till systemägaren,

e) förvalta och hantera produkter för kryptering, och därvid säkerställa förvaringen av kryptering och kontrollerat material samt, i förekommande fall, framställningen av kryptografiska variabler,

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

g) tillhandahålla systemspecifik utbildning i informationssäkring, och

h) genomföra och svara för driften av systemspecifika säkerhetsåtgärder.

BILAGA V

INDUSTRISÄKERHET

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 11. Här fastställs allmänna säkerhetsbestämmelser för företag eller andra enheter vid kontraktsförhandlingar och under hela löptiden för av generalsekretariatet tilldelade kontrakt som kräver säkerhetsskyddsavtal.

2. Rådet ska godkänna riktlinjer för industrisäkerhet som särskilt innehåller detaljerade krav för säkerhetsgodkännanden av verksamhetsställe, säkerhetsskyddsöverenskommelser, besök, samt överföring och befordran av säkerhetsskyddsklassificerade EU-uppgifter.

II. SÄKERHETSINSLAG I ETT KONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL

Handbok om säkerhetsklassificering

3. Före ett anbudsförfarande eller tilldelningen av ett kontrakt ska generalsekretariatet i egenskap av upphandlande myndighet fastställa säkerhetsklassificeringen för alla uppgifter som ska lämnas ut till anbudsgivare och entreprenörer, och även säkerhetsklassificeringen av eventuella uppgifter från entreprenören. Generalsekretariatet ska i detta syfte utarbeta en handbok om säkerhetsklassificering, som ska användas när kontraktet fullgörs.

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

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

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

c) Där så är lämpligt ska generalsekretariatet utbyta information med medlemsstaternas nationella säkerhetsmyndigheter/utsedda säkerhetsmyndigheter eller andra berörda behöriga säkerhetsmyndigheter i samband med ändringar av säkerhetsskyddsklassificeringsnivån på uppgifter som härrör från eller har lämnats till entreprenören för fullgörandet av kontraktet och för efterföljande ändringar av handboken.

Säkerhetsskyddsöverenskommelse

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

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

Säkerhetsanvisningar för program/projekt

7. Beroende på omfattningen av program eller projekt som innebär tillgång till eller hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter kan särskilda säkerhetsanvisningar för program/projekt utarbetas av den upphandlande myndighet som utsetts för att förvalta programmet eller projektet. Säkerhetsföreskrifterna för program/projekt ska godkännas av medlemsstaternas nationella säkerhetsmyndigheter/utsedda säkerhetsmyndigheter eller annan behörig säkerhetsmyndighet som deltar i programmet/projektet och kan innehålla ytterligare säkerhetskrav.

III. SÄKERHETSGODKÄNNANDE AV VERKSAMHETSSTÄLLE

8. Ett säkerhetsgodkännande av verksamhetsställe ska beviljas av en medlemsstats nationella säkerhetsmyndighet, utsedda säkerhetsmyndighet eller annan behörig säkerhetsmyndighet som en indikation på, i enlighet med nationella lagar och andra författningar, att en industrienhet eller en annan enhet kan skydda säkerhetsskyddsklassificerade EU-uppgifter med lämplig säkerhetsskyddsklassificeringsnivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) inom sina anläggningar. Det ska läggas fram för generalsekretariatet i egenskap av upphandlande myndighet, innan en entreprenör eller underentreprenör, eller potentiella sådana, kan få eller beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

9. När en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet utfärdar ett säkerhetsgodkännande av verksamhetsställe ska den, som ett minimum,

a) utvärdera integriteten hos industrienheten eller varje annan enhet,

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

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

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

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

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

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

12. Den nationella/utsedda säkerhetsmyndighet eller annan behörig säkerhetsmyndighet som har utfärdat ett säkerhetsgodkännande av verksamhetsställe ska meddela generalsekretariatet i egenskap av upphandlande myndighet om alla ändringar som avser detta godkännande. När det gäller underentreprenader ska den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet informeras i enlighet med detta.

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

IV. KONTRAKT OCH UNDERENTREPRENÖRSKONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL

14. När säkerhetsskyddsklassificerade EU-uppgifter lämnas till en anbudsgivare i det förkontraktuella skedet ska meddelandet om upphandling innehålla en bestämmelse som förpliktigar den anbudsgivare som inte lämnat något anbud eller valts ut att inom en bestämd tid återlämna alla säkerhetsskyddsklassificerade handlingar.

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

16. När sådana kontrakt sägs upp ska generalsekretariatet, i egenskap av upphandlande myndighet (och/eller den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet, beroende på vad som är lämpligt när det gäller underentreprenader), omedelbart underrätta den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet i den medlemsstat där entreprenören eller underentreprenören är registrerad.

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

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

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

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

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

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

23. När det gäller säkerhetsskyddsklassificerade EU-uppgifter som upprättats eller hanterats av entreprenören eller underentreprenören ska upphovsmannens rättigheter utövas av den upphandlande myndigheten.

V. BESÖK MED ANKNYTNING TILL KONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL

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

25. Alla besökare ska inneha ett lämpligt personalsäkerhetsgodkännande och ha behovsenlig behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter med anknytning till generalsekretariatets kontrakt.

26. Besökare ska enbart ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter som har samband med besökets syfte.

VI. ÖVERFÖRING OCH BEFORDRAN AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

27. Överföringen av säkerhetsskyddsklassificerade EU-uppgifter på elektronisk väg ska omfattas av tillämpliga bestämmelser i artikel 10 och bilaga IV.

28. När det gäller befordran av säkerhetsskyddsklassificerade EU-uppgifter ska tillämpliga bestämmelser i bilaga III gälla, i enlighet med nationella lagar och andra författningar.

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

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

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

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

d) Innan något material på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET förflyttas över en gräns ska avsändaren upprätta en transportplan som ska godkännas av den nationella/utsedda säkerhetsmyndigheten eller av någon annan berörd behörig säkerhetsmyndighet.

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

f) När så är möjligt ska rutterna helt och hållet förläggas inom medlemsstaterna. Rutter som går genom andra stater än medlemsstater bör endast användas efter tillstånd från den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet i både den avsändande och den mottagande staten.

VII. ÖVERFÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER TILL ENTREPRENÖRER I TREDJESTATER

30. Säkerhetsskyddsklassificerade EU-uppgifter ska överföras till entreprenörer och underentreprenörer i tredjestater i enlighet med säkerhetsbestämmelser som överenskommits mellan generalsekretariatet, i egenskap av upphandlande myndighet, och den nationella/utsedda säkerhetsmyndigheten i den berörda tredjestat där entreprenören är registrerad.

VIII. UPPGIFTER PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅN RESTREINT UE/EU RESTRICTED

31. Tillsammans med medlemsstatens nationella/utsedda säkerhetsmyndighet ska generalsekretariatet i egenskap av upphandlande myndighet, när så är lämpligt, ha rätt att i enlighet med kontraktsbestämmelserna inspektera entreprenörens/underentreprenörens verksamhetsställen för att kontrollera att de nödvändiga säkerhetsåtgärder för skydd av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED som krävs enligt kontraktet har vidtagits.

32. I den omfattning som krävs enligt nationella lagar och andra författningar ska rådets generalsekretariat såsom den upphandlande myndigheten underrätta de nationella/utsedda säkerhetsmyndigheterna eller annan behörig säkerhetsmyndighet om kontrakt och underentreprenörskontrakt som innehåller uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

33. Det krävs inte något säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande för entreprenörer eller underentreprenörer och deras personal för kontrakt som tilldelas av generalsekretariatet och som innehåller uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

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

35. De villkor enligt vilka entreprenören får lägga ut kontrakt på underentreprenad ska överensstämma med punkt 21.

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

BILAGA VI

UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER MED TREDJESTATER OCH INTERNATIONELLA ORGANISATIONER

I. INLEDNING

1. Denna bilaga innehåller tillämpningsbestämmelser för artikel 13.

II. RAMAR SOM GÄLLER FÖR UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

2. Om rådet fastställer att det finns ett långvarigt behov av utbyte av säkerhetsskyddsklassificerade uppgifter ska

— ett informationssäkerhetsavtal ingås, eller

— en administrativ överenskommelse ingås,

i enlighet med artikel 13.2 och avsnitten III och IV och på grundval av en rekommendation från säkerhetskommittén.

3. När säkerhetsskyddsklassificerade EU-uppgifter som framställts för en GSFP-insats ska tillhandahållas tredjestater eller internationella organisationer som deltar i sådana insatser, och när ingen av ramarna i punkt 2 föreligger, ska utbytet av säkerhetsskyddsklassificerade EU-uppgifter med den bidragande tredjestaten eller internationella organisationen regleras i enlighet med avsnitt V genom

— ett ramavtal om deltagande,

— ett ad hoc-avtal om deltagande, eller

— avsaknad av något av ovanstående, en administrativ ad hoc-överenskommelse.

4. Om det inte finns någon sådan ram som avses i punkterna 2 och 3, och när ett beslut fattas om att utlämna säkerhetsskyddsklassificerade EU-uppgifter till en tredjestat eller internationell organisation i undantagsfall på ad hoc-basis, i enlighet med avsnitt VI, ska den berörda tredjestaten eller internationella organisationen uppmanas att skriftligen försäkra att den ska skydda alla säkerhetsskyddsklassificerade EU-uppgifter som utlämnas i enlighet med de grundprinciper och miniminormer som fastställs i detta beslut.

III. INFORMATIONSSÄKERHETSAVTAL

5. Genom informationssäkerhetsavtal ska grundprinciper och miniminormer fastställas för utbyte av säkerhetsskyddsklassificerade uppgifter mellan unionen och en tredjestat eller internationell organisation.

6. Informationssäkerhetsavtal ska innehålla tekniska genomförandebestämmelser som ska godkännas av behöriga säkerhetsmyndigheter vid relevanta unionsinstitutioner och -organ och den berörda tredjestatens eller internationella organisationens behöriga säkerhetsmyndighet. Sådana bestämmelser ska ta hänsyn till den skyddsnivå som erbjuds genom befintliga säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden i den berörda tredjestaten eller internationella organisationen. De ska godkännas av säkerhetskommittén.

7. Säkerhetsskyddsklassificerade EU-uppgifter får inte utbytas i elektronisk form enligt ett informationssäkerhetsavtal, såvida detta inte uttryckligen föreskrivs i avtalet eller i de motsvarande tekniska genomförandebestämmelserna.

8. När rådet ingår ett informationssäkerhetsavtal med en tredje part ska en registreringsenhet utses hos varje part som huvudsaklig kontaktpunkt för in- och utpassering av säkerhetsskyddsklassificerade uppgifter.

9. För att bedöma ändamålsenligheten av säkerhetsbestämmelserna, säkerhetsstrukturerna och säkerhetsförfarandena i den berörda tredjestaten eller internationella organisationen ska utvärderingsbesök genomföras i samförstånd med den berörda tredjestaten eller internationella organisationen. Utvärderingsbesöken ska genomföras i enlighet med relevanta bestämmelser i bilaga III och innebära en utvärdering av

a) det regelverk som ska tillämpas för skyddet av säkerhetsskyddsklassificerade uppgifter,

b) eventuella särdrag i säkerhetsstrategin och metoderna för organisering av säkerheten i tredjestaten eller den internationella organisationen som kan påverka säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade uppgifter som får utbytas,

c) de säkerhetsåtgärder och säkerhetsförfaranden som faktiskt har införts, och

d) förfarandena för säkerhetsprövning motsvarande säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som ska lämnas ut.

10. Den grupp som genomför utvärderingsbesök på unionens vägnar ska bedöma om säkerhetsbestämmelserna och säkerhetsförfarandena i den berörda tredjestaten eller internationella organisationen är tillräckliga för att skydda säkerhetsskyddsklassificerade EU-uppgifter på en viss nivå.

11. Resultaten av besöken ska redovisas i en rapport, på grundval av vilken säkerhetskommittén ska fastställa den övre säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får utlämnas som pappers-kopia, och eventuellt elektroniskt, till den berörda tredje parten samt eventuella särskilda villkor för utbytet med den parten.

12. Allt ska göras för att ett fullständigt säkerhetsutvärderingsbesök ska kunna genomföras hos den berörda tredjestaten eller internationella organisationen, så att det går att klargöra det befintliga säkerhetssystemets egenskaper och effektivitet, innan säkerhetskommittén godkänner genomförandebestämmelserna. Om detta visar sig vara omöjligt ska säkerhetskommittén erhålla en så fullständig rapport som möjligt från generalsekretariatets säkerhetsavdelning grundad på den information denna har tillgång till, för att upplysa säkerhetskommittén om de tillämpliga säkerhets-bestämmelserna och det sätt på vilket säkerheten organiseras hos den berörda tredjestaten eller internationella organisationen.

13. Rapporten om utvärderingsbesöket eller, vid avsaknad av en sådan rapport, den rapport som avses i punkt 12, ska översändas till och godkännas av säkerhetskommittén innan några säkerhetsskyddsklassificerade EU-uppgifter lämnas ut till den berörda tredjestaten eller internationella organisationen.

14. Behöriga säkerhetsmyndigheter vid unionens institutioner och organ ska meddela tredjestaten eller den internationella organisationen om vilken dag unionen kan börja lämna ut säkerhetsskyddsklassificerade EU-uppgifter enligt avtalet och om den övre säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får lämnas ut i pappersformat eller elektroniskt.

15. Uppföljningsbesök ska genomföras vid behov, särskilt om

a) det finns behov av att höja säkerhetsskyddsklassificeringsnivån för vilka säkerhetsskyddsklassificerade EU-uppgifter som kan lämnas ut,

b) Unionen har informerats om grundläggande ändringar av tredjestatens eller den internationella organisationens säkerhetsarrangemang som skulle kunna inverka på hur den skyddar säkerhetsskyddsklassificerade EU-uppgifter eller

c) en allvarlig incident har inträffat som inbegriper obehörigt röjande av säkerhetsskyddsklassificerade EU-uppgifter.

16. När informationssäkerhetsavtalet har trätt i kraft och säkerhetsskyddsklassificerade uppgifter utbyts med den berörda tredjestaten eller internationella organisationen, får säkerhetskommittén besluta att ändra den högsta säkerhetsskydds-klassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får lämnas ut i pappersform eller i elektronisk form, särskilt mot bakgrund av ett uppföljande utvärderingsbesök.

IV. ADMINISTRATIVA ÖVERENSKOMMELSER

17. När det föreligger ett långsiktigt behov av att utbyta säkerhetsskyddsklassificerade uppgifter som i regel inte ligger över säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED med en tredjestat eller internationell or-ganisation, och när säkerhetskommittén har fastställt att den parten inte har ett tillräckligt utvecklat säkerhetssystem för att ingå ett informationssäkerhetsavtal, får generalsekreteraren, med förbehåll för rådets godkännande, ingå en administrativ överenskommelse på generalsekretariatets vägnar med de berörda myndigheterna i den aktuella tredje-staten eller internationella organisationen.

18. När ramar för utbyte av säkerhetsskyddsklassificerade EU-uppgifter snabbt behöver införas av operativa skäl, får rådet undantagsvis besluta att en administrativ överenskommelse ska ingås för utbyte av information på en högre säker-hetsskyddsklassificeringsnivå.

19. Administrativa överenskommelser ska i princip ha formen av en skriftväxling.

20. Ett utvärderingsbesök enligt punkt 9 ska genomföras och rapporten eller, vid avsaknad av en sådan rapport, den rapport som avses i punkt 12, ska översändas till och godkännas av säkerhetskommittén innan några säkerhets-skyddsklassificerade EU-uppgifter lämnas ut till den berörda tredjestaten eller internationella organisationen.

21. Inga säkerhetsskyddsklassificerade EU-uppgifter får utbytas på elektronisk väg enligt en administrativ överenskom-melse, såvida detta inte uttryckligen föreskrivs i överenskommelsen.

V. UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER I SAMBAND MED GSFP-INSATSER

22. Ramavtal om deltagande reglerar tredjestaters eller internationella organisationers deltagande i GSFP-insatser. Sådana avtal ska inkludera bestämmelser om utlämning av säkerhetsskyddsklassificerade EU-uppgifter som framställts för GSFP-insatser till de bidragande tredjeländerna eller internationella organisationerna. Den högsta säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får utbytas ska vara RESTREINT UE/EU RESTRICTED för civila GSFP-insatser och CONFIDENTIEL UE/EU CONFIDENTIAL för militära GSFP-insatser, såvida inte något annat anges i det beslut genom vilket varje GSFP-insats upprättas.

23. Ad hoc-avtal om deltagande som ingås för en särskild GSFP-insats ska inkludera bestämmelser om utlämning av säkerhetsskyddsklassificerade EU-uppgifter som framställts för den insatsen till den bidragande tredjestaten eller internationella organisationen. Den högsta säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får utbytas ska vara RESTREINT UE/EU RESTRICTED för civila GSFP-insatser och CONFIDENTIEL UE/EU CONFIDENTIAL för militära GSFP-insatser, såvida inte något annat anges i det beslut genom vilket varje GSFP-insats upprättas.

24. Vid avsaknad av informationssäkerhetsavtal och i väntan på ingående av ett avtal om deltagande ska utlämning av säkerhetsskyddsklassificerade EU-uppgifter som framställts för insatsen till en tredjestat eller internationell organisation som deltar i insatsen ske i enlighet med en administrativ överenskommelse som ska ingås av den höga representanten eller efter ett beslut om ad hoc-utlämning i enlighet med avsnitt VI. Säkerhetsskyddsklassificerade EU-uppgifter ska endast utbytas i enlighet med sådana överenskommelser så länge tredjestaten eller den internationella organisationen fortfarande planeras delta. Den högsta säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter som får utbytas ska vara RESTREINT UE/EU RESTRICTED för civila GSFP-insatser och CONFIDENTIEL UE/EU CONFIDENTIAL för militära GSFP-insatser, såvida inte något annat anges i det beslut genom vilket varje GSFP-insats upprättas.

25. I de bestämmelser om säkerhetsskyddsklassificerade uppgifter som ska ingå i ramavtal om deltagande, ad hoc-avtal om deltagande och administrativa ad hoc-överenskommelser som det hänvisas till i punkterna 22–24 ska det föreskrivas att den berörda tredjestaten eller internationella organisationen ser till att dess personal som avdelats för eventuella insatser skyddar säkerhetsskyddsklassificerade EU-uppgifter i enlighet med rådets säkerhetsbestämmelser och ytterligare riktlinjer utfärdade av de behöriga myndigheterna, inbegripet insatsens befälsordning.

26. Om ett informationssäkerhetsavtal därefter ingås mellan unionen och en bidragande tredjestat eller internationell organisation, ska informationssäkerhetsavtalet ha företräde framför bestämmelserna om utbyte av säkerhetsskyddsklassificerade uppgifter i ett eventuellt ramavtal om deltagande, ett ad hoc-avtal om deltagande eller en administrativ ad hoc-överenskommelse när det gäller utbyte och hantering av säkerhetsskyddsklassificerade EU-uppgifter.

27. Utbyte av säkerhetsskyddsklassificerade EU-uppgifter på elektronisk väg ska inte tillåtas enligt ett ramavtal om deltagande, ett ad hoc-avtal om deltagande eller en administrativ ad hoc-överenskommelse med en tredjestat eller internationell organisation, såvida inte detta uttryckligen föreskrivs i det avtal eller den överenskommelse som berörs.

28. Säkerhetsskyddsklassificerade EU-uppgifter som har framställts för en GSFP-insats får lämnas ut till personal som avdelats för denna insats av tredjestater och internationella organisationer i enlighet med punkterna 22–27. När sådan personal beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter i en GSFP-insats, lokaler eller i kommunikations- och informationssystem, ska åtgärder vidtas (däribland registrering av säkerhetsskyddsklassificerade EU-uppgifter som lämnas ut) för att minska risken för att uppgifter förloras eller röjs. Sådana åtgärder ska fastställas i relevanta planerings- eller uppdragshandlingar.

29. Vid avsaknad av informationssäkerhetsavtal får utlämning av säkerhetsskyddsklassificerade EU-uppgifter till den värdstat på vars territorium GSFP-insatsen genomförs, om det föreligger ett bestämt och omedelbart operativt behov, ske i enlighet med en administrativ överenskommelse som ska ingås av den höga representanten. Denna möjlighet ska föreskrivas i beslutet om GSFP-insatsens inrättande. De säkerhetsskyddsklassificerade EU-uppgifter som lämnas ut under sådana omständigheter får endast vara sådana som framställts för GSFP-insatsen och är placerade på en säkerhetsskyddsklassificeringsnivå som inte överstiger RESTREINT UE/EU RESTRICTED, såvida inte en högre säkerhetsskyddsklassificeringsnivå föreskrivs i beslutet om GSFP-insatsens inrättande. Enligt en sådan administrativ överenskommelse ska värdstaten vara tvungen att åta sig att skydda säkerhetsskyddsklassificerade EU-uppgifter enligt miniminormer som är minst lika stränga som dem som fastställs i detta beslut.

30. Vid avsaknad av informationssäkerhetsavtal får utlämning av säkerhetsskyddsklassificerade EU-uppgifter till relevanta tredjestater och internationella organisationer som inte deltar i GSFP-insatsen ske i enlighet med en administrativ överenskommelse som ska ingås av den höga representanten. Denna möjlighet, liksom eventuella villkor för den, ska i förekommande fall föreskrivas i beslutet om GSFP-insatsens inrättande. De säkerhetsskyddsklassificerade EU-uppgifter som lämnas ut under sådana omständigheter får endast vara sådana som framställts för GSFP-insatsen och är placerade på en säkerhetsskyddsklassificeringsnivå som inte överstiger RESTREINT UE/EU RESTRICTED, såvida inte en högre säkerhetsskyddsklassificeringsnivå föreskrivs i beslutet om GSFP-insatsens inrättande. Enligt en sådan administrativ överenskommelse ska den berörda tredjestaten eller internationella organisationen vara tvungen att åta sig att skydda säkerhetsskyddsklassificerade EU-uppgifter enligt miniminormer som är minst lika stränga som dem som fastställs i detta beslut.

31. Inga arrangemang för genomförande eller utvärderingsbesök krävs före genomförandet av bestämmelserna om utlämning av säkerhetsskyddsklassificerade EU-uppgifter inom ramen för punkterna 22, 23 och 24.

VI. AD HOC-UTLÄMNING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER I UNDANTAGSFALL

32. Om inga ramar har inrättats i enlighet med avsnitten III–V och om rådet eller ett av dess förberedande organ slår fast att det finns ett exceptionellt behov av att lämna ut säkerhetsskyddsklassificerade EU-uppgifter till en tredjestat eller en internationell organisation, ska generalsekretariatet

a) i möjligaste mån med den berörda tredjestatens eller internationella organisationens säkerhetsmyndigheter kontrollera att dess säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden garanterar att de säkerhetsskyddsklassificerade EU-uppgifter som kommer att lämnas ut till denna skyddas enligt normer som är minst lika stränga som dem som fastställs i detta beslut, och

b) uppmana säkerhetskommittén att utifrån tillgänglig information utfärda en rekommendation om tillförlitligheten i säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden i den tredjestat eller internationella organisation dit säkerhetsskyddsklassificerade EU-uppgifter ska lämnas ut.

33. Om säkerhetskommittén utfärdar en rekommendation att lämna ut säkerhetsskyddsklassificerade EU-uppgifter, ska ärendet föreläggas Coreper för beslut om sådan utlämning.

34. Om säkerhetskommittén i sin rekommendation inte tillstyrker att de säkerhetsskyddsklassificerade EU-uppgifterna lämnas ut ska

a) kommittén för utrikes- och säkerhetspolitik, i frågor som rör Gusp/GSFP, diskutera ärendet och utarbeta en rekommendation till Corepers beslut,

b) Coreper, i alla övriga frågor, diskutera ärendet och fatta ett beslut.

35. Om det bedöms vara lämpligt och upphovsmannen i förväg och i skriftlig form lämnar sitt samtycke till detta, får Coreper besluta att de säkerhetsskyddsklassificerade uppgifterna endast delvis får lämnas ut eller endast om de först placeras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre ska vara säkerhetsskyddsklassificerade, eller att de ska lämnas ut utan hänvisning till källan eller den ursprungliga EU-säkerhetsskyddsklassificeringsnivån.

36. Efter ett beslut om att lämna ut säkerhetsskyddsklassificerade EU-uppgifter ska generalsekretariatet översända den berörda handlingen, som ska ha en markering om att uppgifterna får lämnas ut samt om vilken tredjestat eller internationell organisation de har lämnats ut till. Före eller vid den faktiska utlämningen ska den berörda tredje parten skriftligen åta sig att skydda de mottagna säkerhetsskyddsklassificerade EU-uppgifterna i enlighet med de grundläggande principer och miniminormer som anges i detta beslut.

VII. BEHÖRIGHET ATT LÄMNA UT SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER TILL TREDJESTATER ELLER INTERNATIONELLA ORGANISATIONER

37. När ramar föreligger i enlighet med punkt 2 för utbyte av säkerhetsskyddsklassificerade uppgifter med en tredjestat eller internationella organisation, ska rådet fatta beslut om att bemyndiga generalsekreteraren att lämna ut säkerhetsskyddsklassificerade EU-uppgifter, i enlighet med principen om upphovsmannens samtycke, till den berörda tredjestaten eller internationella organisationen. Generalsekreteraren får delegera sådana bemyndiganden till högre tjänstemän vid generalsekretariatet.

38. När ett informationssäkerhetsavtal föreligger i enlighet med punkt 2 första strecksatsen får rådet fatta beslut om att bemyndiga den höga representanten att lämna ut säkerhetsskyddsklassificerade EU-uppgifter som upprättats av rådet på området för den gemensamma utrikes- och säkerhetspolitiken till den berörda tredjestaten eller internationella organisationen, efter att ha erhållit samtycke från upphovsmannen till allt eventuellt ingående källmaterial. Den höga representanten får delegera sådana bemyndiganden till högre tjänstemän vid Europeiska utrikestjänsten eller till EU:s särskilda representanter.

39. När ramar föreligger i enlighet med punkt 2 eller punkt 3 för utbyte av säkerhetsskyddsklassificerade uppgifter med en tredjestat eller internationell organisation, ska den höga representanten bemyndigas att lämna ut säkerhetsskyddsklassificerade EU-uppgifter, i enlighet med beslutet om inrättande av GSFP-insatsen och med principen om upphovsmannens samtycke. Den höga representanten får delegera sådana bemyndiganden till högre tjänstemän vid Europeiska utrikestjänsten, EU-insatsen, styrke- eller uppdragschefer eller till EU:s beskickningschefer.

Tillägg

Tillägg A

Definitioner

Tillägg B

Jämförelsetabell för säkerhetsskyddsklassificeringsnivåer

Tillägg C

Förteckning över nationella säkerhetsmyndigheter

Tillägg D

Förteckning över förkortningar

Tillägg A

DEFINITIONER

I detta beslut avses med

ackreditering: en process som leder fram till ett formellt uttalande från ackrediteringsmyndigheten för säkerhet om att ett system har godkänts för drift med en fastställd sekretessgrad, i en särskild säker driftsform inom sin driftsmiljö och med en godtagbar risknivå på grundval av antagandet att godkända tekniska, fysiska, organisatoriska och förfarandemässiga säkerhetsåtgärder har genomförts,

tillgång: allt av värde för en organisation, dess affärsrörelse och deras fortbestånd, inklusive informationsresurser som stöder organisationens uppdrag,

behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter: ett beslut som generalsekretariatets tillsättningsmyndighet fattat på grundval av en positiv bedömning från den behöriga myndigheten i en medlemsstat om att en tjänsteman eller annan anställd vid generalsekretariatet eller en nationell expert, under förutsättning att personens behovsenliga behörighet har fastställts och denne har fått vederbörlig information om sitt ansvar, beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum,

livscykel för kommunikations- och informationssystem: systemens hela existenstid, inbegripet inledande initiativ, grundidé, planering, kravanalys, utformning, utveckling, testning, genomförande, drift, underhåll och avveckling,

kontrakt som kräver säkerhetsskyddsavtal: ett kontrakt som ingås av rådets generalsekretariat med en entreprenör om leverans av varor, utförande av arbete eller tillhandahållande av tjänster, där genomförandet kräver eller innebär tillgång till eller upprättande av säkerhetsskyddsklassificerade EU-uppgifter,

underentreprenörskontrakt som kräver säkerhetsskyddsavtal: ett kontrakt som ingås av generalsekretariatets entreprenör med en annan entreprenör (dvs. underentreprenör) om leverans av varor, utförande av arbete eller tillhandahållande av tjänster där genomförandet kräver eller innebär tillgång till eller framställande av säkerhetsskyddsklassificerade EU-uppgifter,

kommunikations- och informationssystem: se artikel 10.2,

entreprenör: en fysisk eller juridisk person som har rättskapacitet att ingå kontrakt,

kryptomaterial: kryptoalgoritmer, maskinvara för kryptering och programvarumoduler, och produkter inklusive tillämpningsdetaljer med tillhörande dokumentation och nyckelmaterial,

kryptoprodukt: en produkt vars främsta och huvudsakliga funktion är tillhandahållandet av säkerhetstjänster (konfidentialitet, riktighet, tillgänglighet, autenticitet och oavvislighet) genom en eller flera krypteringsmekanismer,

GSFP-insats: en militär eller civil krishanteringsinsats inom avdelning V kapitel 2 i EU-fördraget,

beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade: borttagande av varje säkerhetsklassificering,

flernivåförsvar: tillämpningen av en rad säkerhetsåtgärder som organiseras som multipla försvarsskikt,

utsedd säkerhetsmyndighet: en myndighet som är ansvarig inför medlemsstatens nationella säkerhetsmyndighet och som ansvarar för att informera industrienheter eller andra enheter om den nationella strategin i alla frågor rörande industrisäkerhet och för att ge ledning och bistånd vid dess genomförande; den utsedda säkerhetsmyndighetens verksamhet får utföras av den nationella säkerhetsmyndigheten eller av någon annan behörig myndighet,

handling: registrerad information, oavsett fysisk form eller egenskaper,

inplacering på lägre säkerhetsskyddsklassificeringsnivå: sänkning av nivån på säkerhetsklassificeringen,

säkerhetsskyddsklassificerade EU-uppgifter: se artikel 2.1,

säkerhetsgodkännande av verksamhetsställe: ett administrativt beslut av en nationell säkerhetsmyndighet eller utsedd säkerhetsmyndighet om att ett verksamhetsställe ur säkerhetsperspektiv är i stånd att erbjuda tillräckligt säkerhetsskydd av säkerhetsskyddsklassificerade EU-uppgifter på en specificerad säkerhetsskyddsklassificeringsnivå,

hantering av säkerhetsskyddsklassificerade EU-uppgifter: all hantering som säkerhetsskyddsklassificerade EU-uppgifter kan utsättas för under hela sin livscykel; detta omfattar deras upprättande, behandling, befordran, inplacering på lägre säkerhetsskyddsklassificeringsnivå, beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade och förstöring; i samband med kommunikations- och informationssystem omfattar detta också insamling, visning, överföring och förvaring,

innehavare: vederbörligen bemyndigad person som konstaterats ha behovsenlig behörighet och som förfogar över en säkerhetsskyddsklassificerad EU-uppgift och därmed ansvarar för dess skydd,

industrienhet eller annan enhet: en enhet som är verksam med att leverera varor, utföra arbeten eller tillhandahålla tjänster; detta kan inbegripa industrienheter och kommersiella enheter samt enheter inom sektorerna för tjänster, vetenskap, forskning, utbildning eller utveckling eller egenföretagare,

industrisäkerhet: se artikel 11.1,

informationssäkring: se artikel 10.1,

sammankoppling: se bilaga IV punkt 32,

hantering av säkerhetsskyddsklassificerade uppgifter: se artikel 9.1,

material: handlingar, databärare eller varje slag av maskin eller utrustning som tillverkats eller håller på att tillverkas,

upphovsman: unionsinstitution, unionsbyrå eller unionsorgan, medlemsstat, tredjestat eller internationell organisation under vilkens behörighet säkerhetsskyddsklassificerade uppgifter har upprättats och/eller införts i unionens strukturer,

personalsäkerhet: se artikel 7.1,

personalsäkerhetsgodkännande: ett uttalande från en medlemsstats behöriga myndighet vilket görs efter genomförande av en säkerhetsprövning som utförs av en medlemsstats behöriga myndigheter och i vilket det intygas att en person får beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum,

intyg om personalsäkerhetsgodkännande: ett intyg utfärdat av en behörig myndighet där det fastställs att en person är säkerhetsprövad och innehar ett giltigt intyg om säkerhetsgodkännande eller av tillsättningsmyndigheten har getts behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter, och som visar vilken nivå av säkerhetsskyddsklassificerade EU-uppgifter som personen ska ha tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), giltighetsdatum för respektive personalsäkerhetsgodkännande samt vilket datum själva intyget löper ut,

fysisk säkerhet: se artikel 8.1,

säkerhetsanvisningar för program/projekt: en förteckning över säkerhetsförfaranden som tillämpas för ett särskilt program/projekt för att standardisera säkerhetsförfaranden; det kan bli föremål för översyn under hela program/projekttiden,

registrering: se bilaga III punkt 18,

kvarstående risk: den risk som kvarstår efter det att säkerhetsåtgärder har genomförts, med tanke på att alla hot inte kan motverkas och att alla sårbarheter inte kan elimineras,

risk: potentialen för att ett givet hot kommer att utnyttja intern och extern sårbarhet hos en organisation eller något av de system den använder och därigenom skada organisationen och dess materiella eller immateriella tillgångar; den kan mätas som en kombination av sannolikheten att hot uppträder och följderna därav,

— *riskacceptans:* ett beslut efter riskhanteringen om att godta att en kvarstående risk fortfarande existerar,

— *riskbedömning:* att identifiera hot och sårbarheter och utföra därmed sammanhängande riskanalys, dvs. en analys av sannolikhet och konsekvenser,

— *riskkommunikation:* att utveckla medvetenheten om risker bland systemanvändargrupper, informera tillståndsmyndigheter om sådana risker och rapportera dem till driftsmyndigheter,

— *riskhantering:* att mildra, undanröja, reducera (genom en lämplig kombination av tekniska, fysiska, organisatoriska eller procedurmässiga åtgärder), överföra eller övervaka risken,

säkerhetsskyddsöverenskommelse: särskilda kontraktsvillkor som utfärdas av den upphandlande myndigheten och som utgör en integrerad del av varje kontrakt som kräver säkerhetsskyddsavtal som innebär tillgång till eller framställande av säkerhetsskyddsklassificerade EU-uppgifter och i vilka säkerhetskraven eller de delar av avtalet som kräver säkerhetsskydd fastställs,

handbok om säkerhetsklassificering: en handling som beskriver de delar av ett program eller kontrakt som är säkerhetsskyddsklassificerade och fastställer de tillämpliga säkerhetsskyddsklassificeringsnivåerna; handboken om säkerhetsklassificering får utökas under programmets eller kontraktets löptid, och delar av uppgifterna kan placeras på en ny eller lägre säkerhetsskyddsklassificeringsnivå; dessa handböcker ska utgöra en del av säkerhetsskyddsöverenskommelsen,

säkerhetsprövning: utredningsförfarande som den behöriga nationella myndigheten genomfört i en medlemsstat i enlighet med sina nationella lagar och andra författningar för att kunna lämna en försäkran om att inget negativt är känt som hindrar att personen ges ett personalsäkerhetsgodkännande eller behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre),

driftsform för säkerhet: definitionen av de förhållanden under vilka ett system drivs baserat på sekretessgrad för de uppgifter som hanteras i systemet och nivåer för godkännande, formellt godkännande för tillgång, och behovsenlig behörighet för dess användare; fyra driftsformer förekommer för hantering eller överföring av sekretessbelagda uppgifter: dedikerad säkerhet, högnivåsäkerhet och flernivåsäkerhet,

— *dedikerad säkerhet:* en driftsform där alla personer som har tillgång till systemet har behörighet för uppgifter med den högsta säkerhetsskyddsklassificeringsnivå som hanteras i systemet och för tjänsteutövningen har behovsenlig behörighet att få tillgång till alla uppgifter som hanteras i systemet,

— *högnivåsäkerhet:* en driftsform där alla personer som har tillgång till kommunikations- och informationssystemet har behörighet för uppgifter på den högsta säkerhetsskyddsklassificeringsnivå som hanteras i systemet, men där inte alla personer som har tillgång till systemet har behovsenlig behörighet att få tillgång till de uppgifter som hanteras i systemet. Godkännande av tillgång till uppgifterna kan göras av en person,

— *kategoriindelad säkerhet:* en driftsform där alla personer som har tillgång till systemet har behörighet för uppgifter på den högsta säkerhetsskyddsklassificeringsnivå som hanteras i systemet, men där inte alla personer som har tillgång till systemet har formell behörighet att få tillgång till alla uppgifter som hanteras i systemet. Formell behörighet innebär en formell central förvaltning av tillgångskontroll till skillnad från en persons skönsmässiga beviljande av tillgång,

— *flernivåsäkerhet:* en driftsform där inte alla personer som har tillgång till systemet har behörighet för uppgifter på den högsta säkerhetsskyddsklassificeringsnivå som hanteras i systemet, och där inte alla personer som har tillgång till systemet har allmän behovsenlig behörighet för de uppgifter som hanteras i systemet,

process för säkerhetsriskhantering: hela processen att fastställa, kontrollera och minimera ovissa händelser som kan påverka säkerheten hos en organisation eller något av de system den använder. Den omfattar all riskrelaterad verksamhet, inklusive bedömning, hantering, acceptans och kommunikation,

tempest: utredning, undersökning och kontroll av komprometterande elektromagnetiska läckor och åtgärder för att upphäva denna,

hot: en potentiell orsak till en oönskad incident som kan ge upphov till skador i en organisation eller något av de system den använder; sådana hot kan vara oavsiktliga eller avsiktliga (uppsåtliga) och kännetecknas av hotande element, potentiella mål och angreppsmetoder,

sårbarhet: alla sorters svagheter som kan utnyttjas genom ett eller flera hot. Sårbarhet kan vara en försummelse eller höra samman med brister i kontrollernas styrka, fullständighet eller konsekvens och kan gälla teknik, förfarande, fysiska förhållanden, organisation eller drift.

Tillägg B

JÄMFÖRELSETABELL FÖR SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅER

EU	TRÈS SECRET/UE EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgien	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	se fotnot (1) nedan
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Tjeckien	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Tyskland	STRENG GEHEIM	GEHEIM	VS (2) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irland	Top Secret	Secret	Confidential	Restricted
Grekland	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spanien	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Frankrike	Très Secret Défense	Secret Défense	Confidentiel Défense	se fotnot (3) nedan
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Cypern	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungern	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted (4)
Nederländerna	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRÈS SECRET/UE EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Rumänien	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenien	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakien	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sverige ([5])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Förenade kungariket	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

([1]) Diffusion Restreinte/Beperkte Verspreiding är inte en säkerhetsskyddsmarkering i Belgien. Belgien hanterar och skyddar uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED på ett sätt som inte är mindre strängt än de normer och förfaranden som anges i säkerhetsbestämmelserna för Europeiska unionens råd.
([2]) Tyskland: VS = Verschlusssache.
([3]) Frankrike använder inte säkerhetsskyddsklassificeringsnivån RESTREINT i sitt nationella system. Frankrike hanterar och skyddar uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED på ett sätt som inte är mindre strängt än de normer och förfaranden som anges i säkerhetsbestämmelserna för Europeiska unionens råd.
([4]) I Maltas fall kan säkerhetsskyddsmarkeringarna vara på antingen maltesiska eller engelska.
([5]) Sverige: Säkerhetsskyddsmarkeringarna i övre raden används av försvarsmyndigheter och de i den undre raden av övriga myndigheter.

Tillägg C

FÖRTECKNING ÖVER NATIONELLA SÄKERHETSMYNDIGHETER

BELGIEN
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bryssel

Tfn sekretariatet +32 25014542
Fax +32 25014596
E-post: nvo-ans@diplobel.fed.be

BULGARIEN
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tfn +359 29333600
Fax +359 29873750
E-post: dksi@government.bg
Internet: www.dksi.bg

TJECKIEN
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Prag 56

Tfn +420 257283335
Fax +420 257283110
E-post: czech.nsa@nbu.cz
Internet: www.nbu.cz

DANMARK
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tfn +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Köpenhamn Ø

Tfn +45 33325566
Fax +45 33931320

TYSKLAND
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin

Tfn +49 30186810
Fax +49 30186811441
E-post: oesIII3@bmi.bund.de

ESTLAND
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tfn +372 7170019, +372 7170117
Fax +372 7170213
E-post: nsa@mod.gov.ee

IRLAND
National Security Authority
Department of Foreign Affairs
76–78 Harcourt Street
Dublin 2

Tfn +353 14780822
Fax +353 14082959

GREKLAND
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Counter Intelligence and Security Directorate (NSA)
227–231 HOLARGOS
STG 1020 Aten

Tfn +30 2106572045
+30 2106572009
Fax +30 2106536279
+30 2106577612

SPANIEN
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tfn +34 913725000
Fax +34 913725808
E-post: nsa-sp@areatec.com

FRANKRIKE
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tfn +33 171758177
Fax +33 171758200

KROATIEN
Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Kroatien

Tfn +385 14681222
Fax +385 14686049
www.uvns.hr

LUXEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxemburg

Tfn +352 24782210 central
+352 24782253 direkt
Fax +352 24782243

ITALIEN
Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Rom

Tfn +39 661174266
Fax +39 64885273

UNGERN
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tfn +36 17952303
Fax +36 17950344
Postal address:
1357 Budapest, PO Box 2
E-post: nbf@nbf.hu
Internet: www.nbf.hu

CYPERN
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22/807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tfn +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-post: cynsa@mod.gov.cy

MALTA
Ministry for Home Affairs and National Security
P.O. Box 146
Valletta

Tfn +356 21249844
Fax +356 25695321

LETTLAND
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001, Riga

Tfn +371 67025418
Fax +371 67025454
E-post: ndi@sab.gov.lv

NEDERLÄNDERNA
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tfn +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tfn +31 703187060
Fax +31 703187522

LITAUEN
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Tfn +370 70666701, +370 70666702
Fax +370 70666700
E-post: nsa@vsd.lt

ÖSTERRIKE
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tfn +43 1531152594
Fax +43 1531152615
E-post: ISK@bka.gv.at

POLEN Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Tfn +48 225857360 Fax +48 225858509 E-post: nsa@abw.gov.pl Internet: www.abw.gov.pl	**SLOVAKIEN** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Tfn +421 268692314 Fax +421 263824005 Internet: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lissabon Tfn +351 213031710 Fax +351 213031711	**FINLAND** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Tfn +358 16055890 Fax +358 916055140 E-post: NSA@formin.fi
RUMÄNIEN Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mureș nr. 4012275 Bukarest Tfn +40 212245830 Fax +40 212240714 E-post: nsa.romania@nsa.ro Internet: www.orniss.ro	**SVERIGE** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS SE-103 39 Stockholm Tfn +46 84051000 Fax +46 87231176 E-post: ud-nsa@foreign.ministry.se
SLOVENIEN Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 SSI-1000 Ljubljana Tfn +386 14781390 Fax +386 14781399 E-post: gp.uvtp@gov.si	**FÖRENADE KUNGARIKET** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Tfn 1: +44 2072765645 Tfn 2: +44 2072765497 Fax +44 2072765651 Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Tillägg D

FÖRTECKNING ÖVER ENGELSKA FÖRKORTNINGAR

Akronym	Betydelse
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems handling EUCI
Coreper	Committee of Permanent Representatives
CSDP	Common Security and Defence Policy
DSA	Designated Security Authority
ECSD	European Commission Security Directorate
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SSRS	System-Specific Security Requirement Statement
TA	TEMPEST Authority

Via EUR-Lex (http://new.eur-lex.europa.eu) har du kostnadsfritt direkt tillgång till Europeiska unionens lagstiftning. På webbplatsen kan du söka i *Europeiska unionens officiella tidning* samt i fördrag, lagstiftning, rättspraxis och förberedande rättsakter.

Mer information om Europeiska unionen finns på http://europa.eu

Europeiska unionens publikationsbyrå
2985 Luxemburg
LUXEMBURG

SV