

Europeiska unionens officiella tidning

C 126



Svensk utgåva

Meddelanden och upplysningar

sextioförsta årgången

10 april 2018

Innehållsförteckning

IV Upplysningar

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER OCH ORGAN

2018/C 126/01

Beslut av unionens höga representant för utrikes frågor och säkerhetspolitik av den 19 september 2017 om Europeiska utrikestjänstens säkerhetsbestämmelser – ADMIN(2017) 10 1

SV

IV

(Upplysningar)

UPPLYSNINGAR FRÅN EUROPEISKA UNIONENS INSTITUTIONER, BYRÅER
OCH ORGAN

EUROPEISKA UTRIKESTJÄNSTEN

**Beslut av unionens höga representant för utrikes frågor och säkerhetspolitik av den 19 september
2017 om Europeiska utrikestjänstens säkerhetsbestämmelser****ADMIN(2017) 10**

(2018/C 126/01)

UNIONENS HÖGA REPRESENTANT FÖR UTRIKES FRÅGOR OCH SÄKERHETSPOLITIK HAR ANTAGIT DETTA BESLUT

med beaktande av rådets beslut 2010/427/EU av den 26 juli 2010 om hur den europeiska avdelningen för yttre åtgärder ska organiseras och arbeta ⁽¹⁾,

med beaktande av yttrandet från den kommitté som avses i artikel 9.6 i den höga representantens beslut av den 15 juni 2011 om säkerhetsbestämmelser för den europeiska avdelningen för yttre åtgärder ⁽²⁾, och

av följande skäl:

- (1) Den europeiska avdelningen för yttre åtgärder (nedan kallad *Europeiska utrikestjänsten* eller *utrikestjänsten*) ska såsom ett i funktionellt hänseende självständigt organ inom Europeiska unionen (EU) ha säkerhetsregler enligt artikel 10.1 rådets beslut 2010/427/EU.
- (2) Unionens höga representant för utrikes frågor och säkerhetspolitik (nedan kallad den höga representanten) bör besluta om säkerhetsbestämmelser för Europeiska utrikestjänsten som ska omfatta alla säkerhetsaspekter på hur utrikestjänsten arbetar, så att den väl kan hantera riskerna för den personal som organisationen ansvarar för och för dess fysiska tillgångar, uppgifter och besökare, och så att den kan fullgöra sina förpliktelser att visa aktsamhet i detta avseende.
- (3) I synnerhet bör skydd erbjudas personal som utrikestjänsten ansvarar för, utrikestjänstens fysiska tillgångar, även kommunikations- och informationssystem, uppgifter och besökare, vilket överensstämmer med bästa praxis i rådet, kommissionen, medlemsstaterna och, i förekommande fall, internationella organisationer.
- (4) Utrikestjänstens säkerhetsbestämmelser bör bidra till att uppnå en mer sammanhängande och heltäckande allmän ram inom EU för skydd av säkerhetsskyddsklassificerade EU-uppgifter, varvid man bygger på och bibehåller en så stor samstämmighet som möjligt med säkerhetsbestämmelserna för Europeiska unionens råd (nedan kallat *rådet*) säkerhetsregler och Europeiska kommissionens säkerhetsbestämmelser.
- (5) Utrikestjänsten, rådet och kommissionen är fast beslutna att tillämpa likvärdiga säkerhetsnormer för skydd av säkerhetsskyddsklassificerade EU-uppgifter.
- (6) Detta beslut påverkar inte artiklarna 15 och 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och tillhörande genomförandeinstrument.

⁽¹⁾ EUT L 201, 3.8.2010, s. 30.

⁽²⁾ EUT C 304, 15.10.2011, s. 7.

- (7) Det är nödvändigt att fastställa hur säkerheten inom utrikestjänsten ska organiseras och hur skyddsuppgifterna ska fördelas inom utrikestjänstens strukturer.
- (8) Den höga representanten bör vid behov stödja sig på relevant expertis i medlemsstaterna, rådets generalsekretariat och i kommissionen.
- (9) Den höga representanten bör, med stöd av medlemsstaterna, rådets generalsekretariat och kommissionen, vidta alla åtgärder som krävs för dessa bestämmelser tillämpning.
- (10) Generalsekreteraren för Europeiska utrikestjänsten är säkerhetsmyndigheten inom utrikestjänsten, och i artikel 1 i beslut ADMIN (2015)34 av den 14 september 2015 från generalsekreteraren för Europeiska avdelningen för yttre åtgärder föreskrivs att säkerhetsmyndighetens säkerhetsfunktioner, enligt Europeiska utrikestjänstens säkerhetsbestämmelser, ska utövas av generaldirektören för budget och administration.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte och tillämpningsområde

I detta beslut fastställs Europeiska utrikestjänstens säkerhetsbestämmelser (nedan kallade *utrikestjänstens säkerhetsbestämmelser*).

Enligt artikel 10.1 i rådets beslut 2010/427/EU av den 26 juli 2010 om hur den europeiska avdelningen för yttre åtgärder ska organiseras och arbeta ska beslutet gälla för utrikestjänstens personal och all personal vid unionens delegationer, oavsett administrativ ställning eller ursprung, och genom beslutet ska ett allmänt regelverk upprättas för att effektivt hantera riskerna för personal som utrikestjänstens ansvarar för i enlighet med artikel 2 samt för utrikestjänstens lokaler, fysiska tillgångar, information och besökare.

Artikel 2

Definitioner

I detta beslut avses med

- a) *utrikestjänstens personal*: tjänstemän och övriga anställda vid utrikestjänsten, inbegripet personal från medlemsstaternas diplomattjänster med tillfällig anställning som nationella experter, enligt definitionen i artikel 6 i rådets beslut 2010/427/EU av den 26 juli 2010 om hur den europeiska avdelningen för yttre åtgärder ska organisera och arbeta.
- b) *personal som utrikestjänsten ansvarar för*: utrikestjänstens personal och all personal vid unionens delegationer, oavsett administrativ ställning eller ursprung, samt, inom ramen för detta beslut, den höga representanten samt, i förekommande fall, övriga personal som är verksam i de lokaler som tillhör utrikestjänstens högkvarter.
- c) *familjemedlemmar*: familjemedlemmar till den personal som utrikestjänsten ansvarar för vid unionens delegationer och som är en del av personalens hushåll i enlighet med anmälan till den mottagande statens utrikesministerium.
- d) *utrikestjänstens lokaler*: utrikestjänstens samtliga anläggningar, inbegripet byggnader, kontor, rum och andra utrymmen, samt utrymmen som inhyser kommunikations- och informationssystem (även system som hanterar säkerhetsskyddsklassificerade EU-uppgifter), där utrikestjänsten bedriver permanent eller tillfällig verksamhet.
- e) *utrikestjänstens säkerhetsintressen*: personal som utrikestjänsten ansvarar för, utrikestjänstens lokaler, familjemedlemmar, fysiska tillgångar, inbegripet kommunikations- och informationssystem, information och besökare.
- f) *säkerhetsskyddsklassificerade EU-uppgifter*: uppgifter eller material som tilldelats en EU-säkerhetsskyddsklassificering och vars obehöriga röjande skulle kunna åsamka olika grader av skada för Europeiska unionens intressen eller för en eller flera av dess medlemsstaters intressen.

- g) *unionsdelegation*: delegationer i tredjeländer och vid internationella organisationer enligt artikel 1.4 i rådets beslut 2010/427/EU av den 26 juli 2010 om hur den europeiska avdelningen för yttre åtgärder ska organiseras och arbeta.

Andra definitioner anges i de relevanta bilagorna och i tillägg A.

Artikel 3

Aktsamhetskrav

1. Utrikestjänstens säkerhetsbestämmelser ska syfta till att utrikestjänsten ska kunna uppfylla sina aktsamhetskrav.
2. Utrikestjänstens aktsamhetskrav omfattar tillbörlig aktsamhet när det gäller att vidta alla rimliga säkerhetsåtgärder för att förhindra att utrikestjänstens säkerhetsintressen skadas på ett sätt som rimligen kan förutses.

Det omfattar både säkerhets- och skyddskomponenter, även de som följer av nödsituationer eller kriser, oavsett deras karaktär.

3. Med beaktande av de aktsamhetskrav som åligger medlemsstater, EU-institutioner eller EU-organ och andra parter med personal i unionens delegationer och/eller de lokaler som tillhör unionens delegationer eller de aktsamhetskrav som åligger utrikestjänsten när unionens delegationer har inhysts i ovannämnda andra parters lokaler, ska utrikestjänsten ingå administrativa överenskommelser med var och en av de ovannämnda enheterna där respektive roller och ansvarsområden samt uppgifter och samarbetsmekanismer ska behandlas.

Artikel 4

Fysisk säkerhet och säkerhet för infrastruktur

1. Utrikestjänsten ska införa alla lämpliga fysiska säkerhetsåtgärder (permanenta eller tillfälliga), inbegripet arrangemang för behörighetskontroll, i alla utrikestjänstens lokaler, för skydd av utrikestjänstens säkerhetsintressen. Vid utformningen och planeringen av nya lokaler eller före hyra av befintliga lokaler ska hänsyn tas till sådana åtgärder.
2. I detta syfte kan särskilda skyldigheter eller begränsningar av säkerhetsskäl åläggas personal som utrikestjänsten ansvarar för och familjemedlemmar, för en viss period och inom särskilda utrymmen.
3. De åtgärder som avses i punkterna 1 och 2 ska stå i proportion till den uppskattade risken.

Artikel 5

Beredskapsnivåer och hantering av krissituationer

1. Europeiska utrikestjänstens säkerhetsmyndighet, såsom denna definieras i artikel 13.1, avsnitt I, ska ansvara för att vidta lämpliga beredskapsåtgärder som förberedelse för eller svar på hot och incidenter som påverkar säkerheten vid Europeiska utrikestjänsten, samt för åtgärder som krävs för att hantera krissituationer.
2. De beredskapsåtgärder som avses i punkt 1 ska stå i proportion till säkerhetshotets omfattning. Nivån på beredskapsåtgärder ska fastställas i nära samarbete med behöriga avdelningar inom andra av unionens institutioner, byråer och organ och med behöriga myndigheter i den medlemsstat eller de medlemsstater där utrikestjänsten har lokaler.
3. Utrikestjänstens säkerhetsmyndighet ska vara kontaktpunkt för frågor om beredskapsnivåer och hantering av krissituationer.

Artikel 6

Skydd av säkerhetsskyddsklassificerade uppgifter

1. Skyddet av säkerhetsskyddsklassificerade EU-uppgifter ska regleras av bestämmelserna i detta beslut och särskilt bilaga A. Innehavare av säkerhetsskyddsklassificerade EU-uppgifter ska vara ansvariga för att skydda dessa uppgifter i enlighet med beslutet.
2. Utrikestjänsten ska se till att tillgång till säkerhetsskyddsklassificerade uppgifter endast beviljas de personer som uppfyller villkoren i artikel 5 i bilaga A.
3. De villkor på vilka lokalanställda kan få tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska också fastställas av den höga representanten, i enlighet med bestämmelserna för skydd av säkerhetsskyddsklassificerade EU-uppgifter i bilaga A till detta beslut.
4. Utrikestjänstens direktorat med ansvar för säkerhet förvaltar en databas om statusen i fråga om personalsäkerhetsgodkännande för alla anställda som utrikestjänsten ansvarar för och entreprenörer som arbetar för utrikestjänsten.
5. Om medlemsstaterna matar in säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsklassificering i utrikestjänstens strukturer eller nät, ska utrikestjänsten skydda uppgifterna i enlighet med kraven för säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå såsom fastställs i tillämpliga bestämmelser i enlighet med tillägg B till detta beslut.
6. Utrymmen inom utrikestjänsten där man förvarar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, eller uppgifter som klassificeras på motsvarande nivå, ska fastställas som säkrade utrymmen i överensstämmelse med bestämmelserna i enlighet med bilaga A II till detta beslut, och ska godkännas av utrikestjänstens säkerhetsmyndighet.
7. Förfaranden för att fullgöra den höga representantens skyldigheter inom ramen för avtal eller administrativa överenskommelser för utbyte av säkerhetsskyddsklassificerade EU-uppgifter med tredjestater eller internationella organisationer beskrivs i bilagorna A och A VI till detta beslut.
8. Generalsekreteraren ska fastställa de villkor enligt vilka utrikestjänstens säkerhetsmyndighet får utbyta säkerhetsskyddsklassificerade EU-uppgifter som den innehar med andra av unionens institutioner, organ, kontor eller byråer. En lämplig ram kommer att inrättas för detta, bland annat genom ingående av interinstitutionella avtal eller andra arrangemang när så krävs.
9. 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 7

Säkerhetsincidenter och nödsituationer

1. För att garantera en snabb och ändamålsenlig reaktion på säkerhetsincidenter ska utrikestjänsten inrätta ett förfarande för rapportering av sådana incidenter och nödsituationer, som ska vara i drift dygnet runt sju dagar i veckan och omfatta alla typer av säkerhetsincidenter eller hot mot utrikestjänstens säkerhetsintressen (t.ex. olyckor, konflikter, sabotage, kriminella handlingar, kidnappnings- och gisslansituationer, medicinska nödsituationer, incidenter avseende kommunikations- och informationssystem, it-angrepp osv.).
2. Sambandskanaler för nödsituationer ska upprättas mellan utrikestjänstens högkvarter, unionens delegationer, rådet, kommissionen, EU:s särskilda representanter och medlemsstaterna för att bistå dem i hanteringen av säkerhetsincidenter som rör personalen och följderna av dessa, inbegripet beredskapsplanering.
3. Denna hantering av säkerhetsincidenter ska bland annat inbegripa följande:
 - Förfaranden för att på bästa sätt stödja beslutsprocessen i samband med en säkerhetsincident som rör personalen, inbegripet beslut rörande indragning eller uppskjutande av ett uppdrag.
 - En strategi och förfaranden för undsättning av personal, t.ex. när det gäller saknad personal eller kidnappnings- och gisslansituationer, med hänsyn till medlemsstaternas, EU-institutionernas och utrikestjänstens särskilda ansvar i detta avseende. Inom ramen för hanteringen av sådan verksamhet ska behovet av särskilda resurser beaktas, med hänsyn till de medel som medlemsstaterna skulle kunna tillhandahålla.

4. Utrikestjänsten ska införa lämpliga administrativa arrangemang för rapportering av säkerhetsincidenter vid unionens delegationer. När så är lämpligt ska medlemsstaterna, kommissionen, andra berörda myndigheter och de berörda säkerhetskommittéerna underrättas.
5. Förfarandena för hantering av incidenter bör övas och ses över regelbundet.

Artikel 8

Säkerhet när det gäller kommunikations- och informationssystem

1. Utrikestjänsten ska skydda den information som hanteras i kommunikations- och informationssystemen mot hot mot dess konfidentialitet, integritet, tillgänglighet, autenticitet och oavvislighet.
2. Bestämmelser, säkerhetsriktlinjer och ett säkerhetsprogram för att skydda alla kommunikations- och informationssystem som ägs eller drivs av utrikestjänsten ska godkännas av utrikestjänstens säkerhetsmyndighet.
3. Bestämmelserna, strategin och programmet ska vara förenliga och genomförandet av dem nära samordnat med rådets och kommissionens bestämmelser, strategier och program och, i förekommande fall, med de säkerhetsstrategier som medlemsstaterna tillämpar.
4. Samtliga kommunikations- och informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter ska genomgå en ackrediteringsprocess. Utrikestjänsten ska tillämpa ett system där hanteringen av säkerhetsackreditering sker i samråd med rådets generalsekretariat och kommissionen.
5. Om skyddet av säkerhetsskyddsklassificerade EU-uppgifter som hanteras av utrikestjänsten tillhandahålls genom kryptoprodukter, ska sådana produkter godkännas av utrikestjänstens kryptogodkännande myndighet på rekommendation av rådets säkerhetskommitté.
6. Utrikestjänstens säkerhetsmyndighet ska, i den utsträckning det är nödvändigt, inrätta följande funktioner för informationssäkring:
 - a) En myndighet för informationssäkring.
 - b) En tempestmyndighet.
 - c) En kryptogodkännande myndighet.
 - d) En kryptodistributionsmyndighet.
7. För varje system ska utrikestjänstens säkerhetsmyndighet inrätta följande funktioner:
 - a) En ackrediteringsmyndighet för säkerhet.
 - b) En driftsansvarig myndighet för informationssäkring.
8. Genomförandebestämmelser för denna artikel med avseende på skyddet av säkerhetsskyddsklassificerade EU-uppgifter anges i bilagorna A och A IV.

Artikel 9

Överträdelser av säkerhetsbestämmelserna och röjande av säkerhetsskyddsklassificerade uppgifter

1. En överträdelse av säkerhetsbestämmelserna inträffar som resultat av en handling eller försummelse och som står i strid med säkerhetsbestämmelserna i detta beslut och/eller de säkerhetsstrategier eller säkerhetsriktlinjer som anger de eventuella åtgärder som är nödvändiga för dess genomförande, som godkänts i enlighet med artikel 21.1.
2. Ett röjande av säkerhetsskyddsklassificerade uppgifter inträffar när uppgifterna helt eller delvis har lämnats ut till obehöriga personer eller enheter.
3. Eventuella överträdelser eller misstänkta överträdelser av säkerhetsbestämmelserna, och eventuellt röjande eller misstänkt röjande av säkerhetsskyddsklassificerade uppgifter ska omedelbart rapporteras till utrikestjänstens direktorat med ansvar för säkerhet, som ska vidta lämpliga åtgärder i enlighet med artikel 11 i bilaga A.
4. En person som är ansvarig för en överträdelse av de säkerhetsbestämmelser som fastställs i detta beslut, eller för röjande av säkerhetsskyddsklassificerade uppgifter, kan bli föremål för disciplinära och/eller rättsliga åtgärder i överensstämmelse med tillämpliga lagar, bestämmelser och andra författningar, i enlighet med artikel 11.3 i bilaga A.

Artikel 10

Utredning av säkerhetsincidenter, överträdelser och/eller röjanden samt korrigerande åtgärder

1. Utan att det påverkar tillämpningen av artikel 86 (Disciplinära förfaranden) och bilaga IX i tjänsteföreskrifterna ⁽¹⁾ får säkerhetsutredningar utföras av Europeiska utrikestjänstens direktorat med ansvar för säkerhet
 - a) vid risk för att säkerhetsskyddsklassificerade EU-uppgifter, sekretessbelagd Euroatom-information eller känsliga icke-sekretessbelagda uppgifter läcks, används på felaktigt sätt eller röjs,
 - b) för att möta angrepp från fientliga underrättelsetjänster som riktar sig mot Europeiska utrikestjänsten och dess personal,
 - c) för att motverka terroristattacker mot Europeiska utrikestjänsten och dess personal,
 - d) vid it-incidenter,
 - e) vid andra händelser som påverkar eller kan påverka den allmänna säkerheten vid Europeiska utrikestjänsten, inklusive misstänkta brott.
2. Europeiska utrikestjänstens direktorat med ansvar för säkerhet, biträtt av experter från medlemsstaterna och/eller från andra EU-institutioner, ska vid behov och när så krävs efter tillstånd från utrikestjänstens säkerhetsmyndighet, vidta alla erforderliga korrigeringsåtgärder som följer av utredningar, när så är lämpligt och på lämpligt sätt.

Endast personal som, med hänsyn till dess aktuella arbetsuppgifter, erhållit ett formellt bemyndigande av utrikestjänstens säkerhetsmyndighet, får ges befogenhet att utföra och samordna säkerhetsutredningar inom Europeiska utrikestjänsten.

3. Utredarna ska ha tillgång till all information som krävs för genomförandet av sådana utredningar och ska få fullt stöd av alla avdelningar och all personal inom utrikestjänsten i detta avseende.

Utredarna får vidta lämpliga åtgärder för att skydda bevis på ett sätt som står i proportion till allvaret hos det ärende som är under utredning.

4. Om tillgången till uppgifter rör personuppgifter, däribland uppgifter i kommunikations- och informationssystem, ska tillgången ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 ⁽²⁾.
5. Om det är nödvändigt att upprätta en utredningsdatabas som innehåller personuppgifter ska Europeiska datatillsynsmannen underrättas i enlighet med nämnda förordning.

Artikel 11

Hantering av säkerhetsrisker

1. För att fastställa sina skyddsbehov ska utrikestjänsten, i nära samarbete med kommissionens säkerhetsdirektorat och vid behov med säkerhetsavdelningen vid rådets generalsekretariat, utarbeta en övergripande metod för bedömning av säkerhetsrisker.
2. Risker för utrikestjänstens säkerhetsintressen ska hanteras som en process. Processen ska syfta till att identifiera kända säkerhetsrisker, fastställa säkerhetsåtgärder som ska minska riskerna till en acceptabel nivå och se till att åtgärderna tillämpas i enlighet med begreppet flernivåförsvar. Verkningsfullheten hos sådana åtgärder, samt graden av risk, ska utvärderas kontinuerligt.

⁽¹⁾ Tjänsteföreskrifter för tjänstemän i Europeiska unionen och anställningsvillkor för övriga anställda i unionen, som fastställs i rådets förordning (EEG, Euratom, EKSG) nr 259/68 (EGT L 56, 4.3.1968, s. 1), nedan kallade *tjänsteföreskrifterna*.

⁽²⁾ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

3. De roller, skyldigheter och uppgifter som fastställs i detta beslut gäller utan att det påverkar ansvarsområdet för varje anställd som utrikestjänsten ansvarar för; särskilt EU-anställda på tjänsteresa i tredjestater måste utöva förnuft och gott omdöme i fråga om den egna säkerheten och följa alla gällande säkerhetsbestämmelser, föreskrifter, förfaranden och instruktioner.
4. I syfte att förebygga och begränsa säkerhetsrisker ska bemyndigad personal ha rätt att utföra säkerhetskontroller på personer som omfattas av detta beslut, för att fastställa huruvida det skulle innebära en säkerhetsrisk att ge dessa personer tillträde till utrikestjänstens lokaler eller tillgång till utrikestjänstens information. För detta ändamål, och i överensstämmelse med förordning (EG) nr 45/2001, får bemyndigad personal a) använda sig av alla informationskällor som är tillgängliga för utrikestjänsten, utan att göra avkall på kravet att kontrollera informationskällans tillförlitlighet, b) skaffa sig tillgång till den personalakt eller de uppgifter i övrigt som utrikestjänsten innehar med avseende på personer som den har anställt eller har för avsikt att anställa, eller med avseende på entreprenörers personal när det är vederbörligen motiverat.
5. Utrikestjänsten ska vidta alla rimliga åtgärder för att se till att dess säkerhetsintressen skyddas och för att förhindra att dessa intressen drabbas av sådan skada som rimligen kan förutses.
6. De säkerhetsåtgärder som vidtas inom utrikestjänsten för att skydda säkerhetsskyddsklassificerade EU-uppgifter under deras livscykel ska särskilt motsvara uppgifternas eller materialets säkerhetsskyddsklassificeringsnivå, form och volym, läget för och konstruktion hos de utrymmen där de säkerhetsskyddsklassificerade EU-uppgifterna förvaras samt hotet, även det lokalt bedömda hotet, från fientlig och/eller brottslig verksamhet, inbegripet spionage, sabotage och terroristverksamhet.

Artikel 12

Säkerhetsmedvetenhet och säkerhetsutbildning

1. Utrikestjänstens säkerhetsmyndighet ska se till att lämpliga program för säkerhetsmedvetenhet och säkerhetsutbildning utformas och genomförs, och att den personal som utrikestjänsten ansvarar för samt, i förekommande fall, deras familjemedlemmar ges den information och den utbildning avseende säkerhetsmedvetenhet som krävs i förhållande till riskerna på deras arbetsplats eller i deras bostad.
2. Personalen ska, innan den ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter och därefter regelbundet, upplysas om och bekräfta att de känner till sitt ansvar att skydda säkerhetsskyddsklassificerade EU-uppgifter i överensstämmelse med bestämmelserna i enlighet med artikel 6.

Artikel 13

Säkerhetsorganisationen inom Europeiska utrikestjänsten

Avsnitt 1

Allmänna bestämmelser

1. Generalsekreteraren ska fungera som utrikestjänstens säkerhetsmyndighet. I denna egenskap ska generalsekreteraren säkerställa följande:
 - a) Att säkerhetsåtgärder samordnas tillsammans med medlemsstaternas behöriga myndigheter, rådets generalsekretariat och Europeiska kommissionen, och i förekommande fall med tredjestaters behöriga myndigheter eller internationella organisationer, efter behov, om alla säkerhetsfrågor av relevans för utrikestjänstens verksamhet, bland annat om arten av risker som hotar utrikestjänstens säkerhetsintressen, och vilka skyddsåtgärder som kan vidtas.
 - b) Att säkerhetsaspekterna beaktas fullt ut redan från början inom utrikestjänstens hela verksamhet.
 - c) Att tillgång till säkerhetsskyddsklassificerade uppgifter endast beviljas till personer som uppfyller villkoren i artikel 5 i bilaga A.
 - d) Att ett registreringssystem inrättas som ska garantera att uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre hanteras i enlighet med detta beslut inom utrikestjänsten, och när de lämnas ut till EU:s medlemsstater, EU:s institutioner, organ eller byråer eller andra godkända mottagare. Ett separat register ska föras över alla de säkerhetsskyddsklassificerade EU-uppgifter som utrikestjänsten lämnar ut till tredjestater och internationella organisationer, och över alla säkerhetsskyddsklassificerade uppgifter som inkommit från tredjestater eller internationella organisationer.
 - e) Att de säkerhetsinspektioner som avses i artikel 16 genomförs.

- f) Att utredningar genomförs av alla eventuella faktiska eller misstänkta överträdelser av säkerhetsbestämmelserna samt av eventuella faktiska eller misstänkta röjanden eller förluster av säkerhetsskyddsklassificerade uppgifter som innehas av eller härrör från utrikestjänsten, och att de berörda säkerhetsmyndigheterna ombes bistå sådana utredningar.
- g) Att lämpliga planer och mekanismer för incident- och konsekvenshantering upprättas så att verkningfulla åtgärder snabbt kan sättas in vid säkerhetsincidenter.
- h) Att lämpliga åtgärder vidtas om personer underlåter att följa detta beslut.
- i) Att lämpliga fysiska och organisatoriska åtgärder vidtas för att skydda utrikestjänstens säkerhetsintressen.

I detta avseende ska utrikestjänstens säkerhetsmyndighet

- fastställa unionsdelegationernas säkerhetskategori, i samråd med kommissionen,
- efter att vid behov ha hört den höga representanten, besluta när unionsdelegationernas personal bör evakueras om säkerhetssituationen så kräver,
- besluta om de åtgärder som ska tillämpas för att vid behov skydda familjemedlemmar, med hänsyn till överenskommelser med EU-institutioner i enlighet med artikel 3.3,
- godkänna policyn för krypterad kommunikation, särskilt programmet för installation av kryptoprodukter och kryptomekanismer.

2. Utrikestjänstens säkerhetsmyndighet ska i denna uppgift biträdas av DGBA, av utrikestjänstens direktör med ansvar för säkerhet och, vid behov, av den biträdande generalsekreteraren för GSFP och krishantering.

3. Generalsekreteraren får som utrikestjänstens säkerhetsmyndighet vid behov delegera uppgifter i detta avseende.

4. Varje avdelningschef/sektionschef ansvarar för genomförandebestämmelserna avseende skyddet för säkerhetsskyddsklassificerade EU-uppgifter i sin avdelning/sektion.

Samtidigt som varje avdelningschef/sektionschef förblir ansvarig enligt ovan ska vederbörande utse personal som ska utöva en funktion som säkerhetssamordnare på avdelningsnivå och vars resurser ska stå i proportion till den mängd säkerhetsskyddsklassificerade EU-uppgifter som den avdelningen/sektionen hanterar.

Säkerhetssamordnarna på avdelningsnivå ska, när så är lämpligt och på lämpligt sätt, bistå och stödja sin avdelningschef/divisionschef i fullgörandet av de uppgifter som har samband med säkerhet, t.ex.

- a) utforma ytterligare säkerhetskrav som är lämpliga med tanke på avdelningens/sektionens särskilda behov,
- b) hålla regelbundna säkerhetsgenomgångar för personalen på sin avdelning/sektion,
- c) se till att principen om behovsenlig behörighet följs på sin avdelning/sektion,
- d) hålla en förteckning över säkra koder och nycklar uppdaterad,
- e) vidmakthålla säkerhetsförfaranden och säkerhetsåtgärder,
- f) rapportera eventuella överträdelser av säkerhetsbestämmelserna och/eller röjande av säkerhetsskyddsklassificerade EU-uppgifter till både direktören och säkerhetsdirektoratet,
- g) genomföra avstämningar med personal som upphör att vara anställda av utrikestjänsten,
- h) lämna regelbundna rapporter via sina överordnade om avdelningens/sektionens säkerhetsfrågor,
- i) hålla kontakt med utrikestjänstens direktorat med ansvar för säkerhet om säkerhetsfrågor.

All verksamhet och alla frågor som kan påverka säkerheten ska i god tid anmälas till utrikestjänstens direktorat med ansvar för säkerhet.

5. Cheferna för unionens delegationer ska ansvara för genomförandet av alla åtgärder som rör säkerheten för unionens delegationer.

Avsnitt 2

Europeiska utrikestjänstens direktorat med ansvar för säkerhet

1. Europeiska utrikestjänsten ska ha ett direktorat med ansvar för säkerhet. Det ska
 - a) förvalta, samordna, övervaka och/eller genomföra alla säkerhetsåtgärder i samtliga lokaler som utrikestjänsten ansvarar för, vid huvudkontoret, i EU och i tredjestater,
 - b) se till att all verksamhet som kan påverka skyddet av utrikestjänstens säkerhetsintressen är förenlig och samstämmig med detta beslut och med genomförandebestämmelserna,
 - c) vara den främste rådgivaren för den höga representanten, utrikestjänstens säkerhetsmyndighet och den biträdande generalsekreteraren när det gäller alla frågor som rör säkerhet,
 - d) biträdas av de behöriga myndigheterna i medlemsstaterna, i enlighet med artikel 10.3 i rådets beslut 2010/427/EU om hur den europeiska avdelningen för yttre åtgärder ska organiseras och arbeta,
 - e) stödja verksamheten vid utrikestjänstens ackrediteringsmyndighet för säkerhet genom att utföra fysiska säkerhetsbedömningar av den allmänna/lokala säkerhetsmiljön för kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter, och för lokaler som ska godkännas för hantering och förvaring av säkerhetsskyddsklassificerade EU-uppgifter.
2. Chefen för utrikestjänstens direktorat med ansvar för säkerhet ska
 - a) sörja för det övergripande skyddet av utrikestjänstens säkerhetsintressen,
 - b) utarbeta, se över och uppdatera säkerhetsbestämmelserna samt samordna säkerhetsåtgärderna med de behöriga myndigheterna i medlemsstaterna och, i förekommande fall, de behöriga myndigheterna i tredjestater och internationella organisationer som är knutna till EU genom säkerhetsavtal och/eller säkerhetsarrangemang,
 - c) bistå vid överläggningarna i utrikestjänstens säkerhetskommitté i enlighet med artikel 15.1 i det här beslutet.
 - d) hålla kontakt med eventuella andra partner eller myndigheter än de som avses i led b om säkerhetsfrågor, när så är lämpligt,
 - e) prioritera och lägga fram förslag för förvaltningen av budgeten för säkerheten i huvudkontoret och vid unionens delegationer.
3. Chefen för utrikestjänstens direktorat med ansvar för säkerhet ska
 - a) se till att överträdelser av säkerhetsbestämmelserna och röjanden registreras och att undersökningar inleds och genomförs om och när så är nödvändigt,
 - b) sammanträda regelbundet och, när så är nödvändigt, diskutera områden av gemensamt intresse med direktören för säkerhetsfrågor vid generalsekretariatet vid rådet och direktören för kommissionens säkerhetsdirektorat.
4. Utrikestjänstens direktorat med ansvar för säkerhet ska upprätta kontakt och upprätthålla ett nära samarbete med
 - de avdelningar som ansvarar för säkerheten vid utrikesministerierna i medlemsstaterna,
 - de nationella säkerhetsmyndigheterna och/eller andra behöriga myndigheter i medlemsstaterna, för att få deras hjälp när det gäller de upplysningar det behöver för att bedöma faror för och hot mot utrikestjänsten, personalen, verksamheten, tillgångarna och resurserna samt dess säkerhetsskyddsklassificerade uppgifter vid den normala verksamhetsorten,
 - de behöriga säkerhetsmyndigheterna i de medlemsstater eller värdstater på vars territorium utrikestjänsten får utöva sin verksamhet, i varje fråga som rör skyddet av personalen, verksamheten, tillgångarna och resurserna samt dess säkerhetsskyddsklassificerade uppgifter,
 - säkerhetsavdelningen vid rådets generalsekretariat och säkerhetsdirektorat vid kommissionens generaldirektorat för personal och säkerhet, och vid behov säkerhetsavdelningarna vid EU:s övriga institutioner, organ och byråer,
 - säkerhetsavdelningarna i tredjestater eller internationella organisationer för möjliga samordningsvinster, och
 - medlemsstaternas nationella säkerhetsmyndigheter, i varje fråga som rör skydd av säkerhetsskyddsklassificerade EU-uppgifter.

Avsnitt 3

Unionens delegationer

1. Varje delegationschef ska ansvara för att lokalt genomföra och sköta alla åtgärder som rör skyddet av utrikestjänstens säkerhetsintressen inom delegationernas lokaler och befogenheter.

Efter att vid behov ha samrått med de behöriga myndigheterna i värdstaten ska han eller hon vidta alla praktiskt genomförbara åtgärder för att se till att lämpliga fysiska och organisatoriska åtgärder genomförs för att uppnå detta mål.

Delegationschefen ska utarbeta säkerhetsförfaranden för skydd av familjemedlemmar enligt definitionen i artikel 2 c, när så är lämpligt, med hänsyn till eventuella administrativa överenskommelser i enlighet med artikel 3.3. Delegationschefen ska rapportera om alla säkerhetsrelaterade frågor inom sitt ansvarsområde till chefen för utrikestjänstens direktorat med ansvar för säkerhet.

Han eller hon ska i dessa uppgifter biträdas av utrikestjänstens direktorat med ansvar för säkerhet, av unionsdelegationens säkerhetsledningsgrupp, som är sammansatt av personal med säkerhetsuppgifter och säkerhetsfunktioner, och av säkerhetspersonal som tjänstgör vid behov.

Unionens delegation ska upprätta regelbundna kontakter och upprätthålla ett nära samarbete i säkerhetsfrågor med medlemsstaternas diplomatiska beskickningar.

2. Dessutom ska delegationschefen

- upprätta detaljerade säkerhets- och beredskapsplaner för delegationen, på grundval av allmänna standardrutiner,
- tillämpa ett verkningsfullt dygnet runt-system för hantering av säkerhetsincidenter och nödsituationer inom delegationens verksamhetsområde,
- se till att all personal som är utstationerad i delegationen har försäkringsskydd enligt vad som krävs för förhållandena i området,
- se till att säkerheten är en del av den introduktionsutbildning vid unionens delegationer som ska ges till all personal före eller vid ankomsten till delegationen, och
- se till att eventuella rekommendationer efter säkerhetsbedömningar genomförs och regelbundet rapporteras skriftligen om genomförandet av dem och om andra säkerhetsfrågor till utrikestjänstens säkerhetsmyndighet.

3. Samtidigt som delegationschefen förblir ansvarig och redovisningsskyldig för att skydda säkerhetsförvaltningen samt för att garantera organisationens återhämtningsförmåga får han eller hon delegera genomförandet av sina säkerhetsuppgifter till delegationens säkerhetssamordnare, dvs. den biträdande delegationschefen eller, om ingen sådan utsetts, en annan lämplig person.

Delegationens säkerhetssamordnare skulle framför allt kunna anförtros följande ansvarsområden:

- Att samordna säkerhetsfunktioner i unionsdelegationen.
- Att upprätthålla kontakt i säkerhetsfrågor med de behöriga myndigheterna i värdlandet och lämpliga motparter vid medlemsstaternas ambassader och diplomatiska beskickningar.
- Att införa lämpliga säkerhetsförvaltningsförfaranden som rör utrikestjänstens säkerhetsintressen, inbegripet skydd av säkerhetsskyddsklassificerade EU-uppgifter.
- Att säkerställa efterlevnad av säkerhetsbestämmelser och säkerhetsinstruktioner.
- Att informera personalen om de säkerhetsbestämmelser som är tillämpliga på dem, samt om de särskilda riskerna i värdlandet.
- Att sända ansökningar till utrikestjänstens direktorat med ansvar för säkerhet om de befattningar som kräver ett personalsäkerhetsgodkännande.
- Att hålla delegationschefen, den regionalt säkerhetsansvarige och utrikestjänstens direktorat med ansvar för säkerhet fortlöpande informerade i fråga om incidenter eller utvecklingen inom området vilka påverkar skyddet av utrikestjänstens säkerhetsintressen.

4. Delegationschefen kan delegera säkerhetsuppgifter av administrativ eller teknisk natur till förvaltningschefen och annan delegationspersonal.

5. Unionens delegation ska biträdas av en regional säkerhetsansvarig. Varje regional säkerhetsansvarig ska utföra de uppgifter som beskrivs nedan vid unionsdelegationen inom sitt geografiska ansvarsområde.

I vissa fall, och om den rådande säkerhetssituationen så kräver, får en särskild regional säkerhetsansvarig förordnas till en särskild delegation på heltidsbasis.

De regionala säkerhetsansvariga kan åläggas att flytta till ett område utanför sitt aktuella ansvarsområde, inklusive huvudkontoret, eller till och med att tillträda en tjänst i vilket land som helst beroende på säkerhetssituationen där, och i enlighet med vad utrikestjänstens direktorat med ansvar för säkerhet kräver.

6. De regionala säkerhetsansvariga ska i operativt hänseende vara direkt underställda den avdelning vid utrikestjänstens huvudkontor som ansvarar för säkerheten på fältet, men stå under administrativ kontroll av delegationschefen på sin anställningsort och huvudkontorets avdelning med ansvar för säkerheten på fältet. De ska bistå delegationschefen och delegationspersonalen vid utarbetandet och genomförandet av alla fysiska, organisatoriska och procedurmässiga åtgärder som avser delegationens säkerhet.

7. De regionala säkerhetsansvariga ger råd och stöd till delegationschefen och delegationspersonalen. Vid behov och särskilt då en regional säkerhetsansvarig arbetar vid en delegation på heltidsbasis, bör han eller hon bistå unionsdelegationen när det gäller säkerhetsförvaltning och genomförande, bl.a. förberedelser för upphandlingar på säkerhetsområdet samt hantering av ackrediteringar och personalsäkerhetsgodkännanden.

Artikel 14

GSFP-insatser och EU:s särskilda representanter

Utrikestjänstens säkerhetsdirektorat bistår och ger råd till direktören för direktoratet för krishantering och planering, generaldirektören för EU:s militära stab (EUMS) och den civila operationschef som leder den civila planerings- och ledningskapaciteten samt befälhavarna för EU:s militära operationer när det gäller säkerhetsaspekterna på GSFP-insatser och EU:s särskilda representanter när det gäller säkerhetsaspekterna av deras uppdrag, som ett komplement till de särskilda bestämmelser som finns i detta avseende i de strategier som rådet antar.

Artikel 15

Utrikestjänstens säkerhetskommitté

1. Härmed inrättas utrikestjänstens säkerhetskommitté.

Kommittén ska ledas av den operativa chefen eller en företrädare som han eller hon utser, och ska sammanträda enligt anvisningar från ordföranden eller på begäran av någon av ledamöterna. Utrikestjänstens säkerhetsdirektorat ska bistå ordföranden i denna funktion och vid behov tillhandahålla administrativt stöd till kommitténs överläggningar.

2. Utrikestjänstens säkerhetskommitté ska vara sammansatt av företrädare för

- varje medlemsstat,
- säkerhetsavdelningen vid rådets generalsekretariat,
- säkerhetsdirektoratet vid kommissionens generaldirektorat för personal och säkerhet.

En medlemsstats delegation till utrikestjänstens säkerhetskommitté kan bestå av ledamöter från

- den nationella säkerhetsmyndigheten och/eller den utsedda säkerhetsmyndigheten,
- de avdelningar som ansvarar för säkerheten vid utrikesministerierna.

3. Kommitténs företrädare får åtföljas och motta råd av experter som de anser nödvändigt. Företrädare för andra av EU:s institutioner, byråer eller organ får bjudas in att delta när frågor som är av betydelse för deras säkerhet diskuteras.

4. Utan att det påverkar tillämpningen av punkt 5 nedan ska utrikestjänstens säkerhetskommitté genom samråd bistå utrikestjänsten när det gäller alla säkerhetsaspekter som är relevanta för utrikestjänstens verksamhet, för huvudkontoret och unionens delegationer.

Utan att det påverkar tillämpningen av punkt 5 nedan gäller för utrikestjänstens säkerhetskommitté särskilt följande:

a) Den ska konsulteras om

- säkerhetsstrategier, riktlinjer, begrepp eller andra metoddokument som rör säkerhet, särskilt i fråga om skyddet av säkerhetsskyddsklassificerade uppgifter och de åtgärder som ska vidtas om utrikestjänstens personal inte iakttar säkerhetsbestämmelserna,
- tekniska säkerhetsaspekter som kan påverka den höga representantens beslut att lägga fram en rekommendation till rådet om att inleda förhandlingar om de informationssäkerhetsavtal som avses i artikel 10.1 a i bilaga A,
- eventuella ändringar av detta beslut.

b) Den kan, beroende på vad som är lämpligt, konsulteras eller underrättas om frågor som rör säkerheten för personal och tillgångar vid utrikestjänstens högkvarter och unionens delegationer, utan att det påverkar tillämpningen av artikel 3.3.

c) Den ska underrättas om eventuella rójanden eller förluster av säkerhetsskyddsklassificerade EU-uppgifter som inträffat inom Europeiska utrikestjänsten.

5. Varje ändring av de bestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter som ingår i detta beslut och dess bilaga A ska kräva ett enhälligt positivt yttrande från medlemsstaterna genom deras företrädare i utrikestjänstens säkerhetskommitté. Ett sådant enhälligt positivt yttrande ska också krävas innan

- förhandlingar inleds om sådana administrativa överenskommelser som avses i artikel 10.1 b i bilaga A,
- säkerhetsskyddsklassificerade uppgifter lämnas ut i de undantagsfall som avses i punkterna 9, 11 och 12 i bilaga A VI,
- ansvaret hos upphovsmannen till uppgifterna övertas under de omständigheter som avses i artikel 10.6 sista meningen i bilaga A.

Om ett enhälligt positivt yttrande begärs kommer detta villkor att uppfyllas om inga invändningar framförs av medlemsstaternas delegationer under kommitténs överläggningar.

6. Utrikestjänstens säkerhetskommitté ska fullt ut beakta de säkerhetsstrategier och säkerhetsriktlinjer som är i kraft i rådet och kommissionen.

7. Utrikestjänstens säkerhetskommitté mottar förteckningen över utrikestjänstens årliga inspektioner, och inspektionsrapporterna, när de har färdigställts.

8. Organisation av sammanträdena:

- Utrikestjänstens säkerhetskommitté ska sammanträda minst två gånger om året. Ytterligare sammanträden, antingen med den fullständiga kommittén eller i ett format med ledamöterna av de nationella/utsedda säkerhetsmyndigheterna eller de avdelningar som ansvarar för säkerheten vid utrikesministerierna, kan anordnas av ordföranden eller begäras av kommitténs ledamöter.
- Utrikestjänstens säkerhetskommitté ska organisera sitt arbete så att den kan lämna rekommendationer inom särskilda områden som gäller säkerhet. Vid behov får den inrätta andra undergrupper med experter. Den ska fastställa mandatet för sådana undergrupper och ta emot deras verksamhetsrapporter.
- Utrikestjänstens direktorat med ansvar för säkerhet ska ansvara för att bereda de frågor som ska behandlas. Ordföranden ska upprätta en preliminär dagordning för varje sammanträde. Kommitténs ledamöter får föreslå ytterligare frågor för diskussion.

*Artikel 16***Säkerhetsinspektioner**

1. Utrikestjänstens säkerhetsmyndighet ska se till att säkerhetsinspektioner görs regelbundet vid utrikestjänstens huvudkontor och i unionens delegationer för att bedöma säkerhetsåtgärdernas lämplighet och kontrollera att de uppfyller kraven i detta beslut. Utrikestjänstens säkerhetsdirektorat får när så är lämpligt utse experter som ska delta i säkerhetsinspektioner vid de EU- byråer och EU-organ som inrättats enligt avdelning V kapitel 2 i EU-fördraget.
2. Utrikestjänstens säkerhetsinspektioner genomförs under ledning av utrikestjänstens säkerhetsdirektorat och, när så är lämpligt, med stöd av säkerhetsexperter som företräder andra EU-institutioner eller medlemsstater, särskilt i samband med de åtgärder som avses i artikel 3.3.
3. Utrikestjänsten får vid behov stödja sig på relevant expertis i medlemsstaterna, rådets generalsekretariat och kommissionen.

Vid behov kan berörda säkerhetsexperter som är baserade i medlemsstaternas representationer i tredjestaterna och/eller företrädare för medlemsstaternas diplomatiska säkerhetsavdelningar bjudas in att delta i säkerhetsinspektionen vid unionsdelegationen.

4. Genomförandebestämmelser för denna artikel med avseende på skyddet av säkerhetsskyddsklassificerade EU-uppgifter anges i bilaga A III.

*Artikel 17***Utvärderingsbesök**

Utvärderingsbesök ska anordnas för att utröna ändamålsenligheten i de säkerhetsåtgärder som tillämpas i en tredjestat eller vid en internationell organisation för att skydda säkerhetsskyddsklassificerade EU-uppgifter som utbyts inom ramen för en administrativ överenskommelse i enlighet med artikel 10.1 b i bilaga A.

Utrikestjänstens direktorat med ansvar för säkerhet får utse experter som ska delta i utvärderingsbesök i tredjestater eller vid internationella organisationer med vilka EU har ingått ett informationssäkerhetsavtal i enlighet med artikel 10.1 a i bilaga A.

*Artikel 18***Planering inför oförutsedda avbrott**

Utrikestjänstens direktorat med ansvar för säkerhet ska bistå utrikestjänstens säkerhetsmyndighet vid förvaltningen av de säkerhetsrelaterade aspekterna på utrikestjänstens processer för oförutsedda avbrott som en del av utrikestjänstens övergripande planering inför oförutsedda avbrott.

*Artikel 19***Reserekommendationer för tjänsteresor utanför EU**

Utrikestjänstens direktorat med ansvar för säkerhet ska garantera tillgången till reserekommendationer när det gäller tjänsteresor utanför EU för personal som utrikestjänsten ansvarar för, och därvid utnyttja resurserna hos alla berörda avdelningar vid utrikestjänsten – särskilt EU:s lägescentral, EU Intcen, de geografiska avdelningarna och unionens delegationer.

Utrikestjänstens direktorat med ansvar för säkerhet ger, på begäran, och med hjälp av ovannämnda resurser, särskilda reserekommendationer för sådana tjänsteresor som anställda som utrikestjänsten ansvarar för företar till tredjestater där hög risk eller förhöjd risknivå föreligger.

*Artikel 20***Hälsa och säkerhet**

Utrikestjänstens säkerhetsbestämmelser kompletterar utrikestjänstens bestämmelser för skydd av hälsa och säkerhet, antagna av den höga representanten.

*Artikel 21***Genomförande och översyn**

1. Utrikestjänstens säkerhetsmyndighet ska, efter samråd med utrikestjänstens säkerhetskommitté, när så är lämpligt godkänna säkerhetsriktlinjer avseende de åtgärder som krävs för genomförandet av dessa bestämmelser vid utrikestjänsten, och ska bygga upp den nödvändiga kapaciteten, som ska täcka alla säkerhetsaspekter, i nära samarbete med medlemsstaternas behöriga säkerhetsmyndigheter och med stöd av berörda myndigheter i EU-institutionerna.
2. I enlighet med artikel 4.5 i rådets beslut 2010/427/EU av den 26 juli 2010 om hur den europeiska avdelningen för yttre åtgärder ska organiseras och arbeta får övergångsbestämmelser användas, vid behov genom servicenivåavtal med berörda avdelningar inom rådets generalsekretariat och kommissionen.
3. Den höga representanten ska sörja för en övergripande enhetlig tillämpning av detta beslut, och ska se till att dessa säkerhetsbestämmelser ses över regelbundet.
4. Utrikestjänstens säkerhetsbestämmelser ska genomföras i nära samarbete med medlemsstaternas behöriga säkerhetsmyndigheter.
5. Utrikestjänsten ska se till att samtliga aspekter av säkerhetsprocessen beaktas inom utrikestjänstens krishanteringsystem.
6. Generalsekreteraren i egenskap av säkerhetsmyndighet och chefen för utrikestjänstens direktorat med ansvar för säkerhet ska ansvara för genomförandet av detta beslut.

*Artikel 22***Ersättande av tidigare beslut**

Detta beslut upphäver och ersätter beslutet av unionens höga representant för utrikes frågor och säkerhetspolitik av den 19 april 2013 om säkerhetsbestämmelser för Europeiska avdelningen för yttre åtgärder ⁽¹⁾.

*Artikel 23***Slutbestämmelser**

Detta beslut träder i kraft samma dag som det undertecknas.

Det ska offentliggöras i *Europeiska unionens officiella tidning*.

De behöriga myndigheterna vid utrikestjänsten ska vederbörligen och i god tid informera all personal som omfattas av detta beslut och dess bilagor, om innehållet i, ikraftträdandet av och eventuella senare ändringar av detta beslut och dess bilagor.

Utfärdat i Bryssel den 19 september 2017.

Federica MOGHERINI

*Unionens höga representant för utrikes frågor och
säkerhetspolitik*

⁽¹⁾ EUT C 190, 29.6.2013, s. 1.

BILAGA A

PRINCIPER OCH NORMER FÖR SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

Artikel 1

Syfte, tillämpningsområde och definitioner

1. I denna bilaga anges de grundläggande principerna och miniminormerna för säkerhet när det gäller skydd av säkerhetsskyddsklassificerade EU-uppgifter.
2. Dessa grundläggande principer och miniminormer ska gälla utrikestjänsten och personal som utrikestjänsten ansvarar för såsom avses och enligt definitionerna i artiklarna 1 och 2 i detta beslut.

Artikel 2

Definition av säkerhetsskyddsklassificerade EU-uppgifter, säkerhetsskyddsklassificering och säkerhetsskyddsmarkeringar

1. Med säkerhetsskyddsklassificerade EU-uppgifter avses 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 följande säkerhetsskyddsklassificeringsnivåer:
 - a) TRES 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. Utrikestjänsten 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 avlägnas utan föregående skriftligt medgivande från upphovsmannen.
3. Utrikestjänstens säkerhetsmyndighet ska, efter samråd med utrikestjänstens säkerhetskommitté enligt artikel 15.5 i detta beslut, godkänna säkerhetsriktlinjer för utarbetande av säkerhetsskyddsklassificerade EU-uppgifter, som ska inbegripa en praktisk vägledning för 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 inför säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsklassificering i utrike tjänstens strukturer eller nät ska utrike tjänsten skydda uppgifterna i enlighet med de krav som gäller för säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå i enlighet med jämförelsetabellen för säkerhetsskyddsklassificeringsnivåer i bilaga B.

Utrike tjänsten ska fastställa lämpliga förfaranden för att föra noggranna register avseende upphovsmannen till

- säkerhetsskyddsklassificerade uppgifter som utrike tjänsten mottar, och
- källmaterial som ingår i säkerhetsskyddsklassificerade uppgifter som upprättats av utrike tjänsten.

Utrike tjänstens säkerhetskommitté ska informeras om dessa förfaranden.

4. Stora mängder eller sammanställningar av säkerhetsskyddsklassificerade EU-uppgifter kan motivera ett skydd som motsvarar en högre säkerhetsskyddsklassificeringsnivå än vad som gäller de enskilda beståndsdelarna.

Artikel 5

Personalsäkerhet för hantering av säkerhetsskyddsklassificerade EU-uppgifter

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, när det gäller tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, har säkerhetsprovats för den berörda nivån, eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar, och
- som har upplysts om sitt ansvar.

2. Genom förfaranden för personalsäkerhetsgodkännande ska det fastställas om en person kan få tillgång till säkerhetsskyddsklassificerad EU-information, med beaktande av vederbörandes lojalitet, tillförlitlighet och pålitlighet.

3. Alla personer ska informeras om och skriftligen bekräfta sitt ansvar när det gäller att skydda säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut innan de ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter och därefter med jämna mellanrum.

4. Genomförandebestämmelser för denna artikel anges i bilaga A I.

Artikel 6

Fysisk säkerhet för säkerhetsskyddsklassificerade EU-uppgifter

1. Med fysisk säkerhet avses tillämpningen av fysiska och tekniska skyddsåtgärder för att avskräcka från 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 behovenlig 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 8.2 i bilaga A.

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

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 anges i bilaga A II.

Artikel 7

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 5, 6 och 8 och därigenom avskräcka, upptäcka och avhjälpa avsiktlig eller oavsiktlig läcka eller förlust av dessa uppgifter. Sådana åtgärder gäller särskilt upprättande, registrering, kopiering, översättning, befordran, hantering, förvaring 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 utrikestjänsten ska i detta syfte inrätta ett registreringssystem. Uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska registreras i de därför avsedda registren.
3. Avdelningar och utrymmen inom vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras ska inspekteras med jämna mellanrum av utrikestjänstens säkerhetsmyndighet.
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 skydd av kryptoprodukter som godkänts i enlighet med artikel 7.5 i detta beslut och enligt klart definierade operativa säkerhetsförfaranden.
 - b) Om de medel som avses i led a inte används ska säkerhetsskyddsklassificerade EU-uppgifter överföras antingen
 - i) elektroniskt (t.ex. USB-minnen, cd-skivor, hårddiskar) som skyddas med kryptoprodukter som godkänts i enlighet med artikel 8.5 i detta beslut, eller
 - ii) i alla övriga fall, som föreskrivet av utrikestjänstens säkerhetsmyndighet i enlighet med de relevanta skyddsåtgärderna i bilaga A III avsnitt V.
5. Genomförandebestämmelser för denna artikel anges i bilaga A III.

Artikel 8

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

1. Med informationssäkring på området kommunikations- och informationssystem avses förvisningar 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. Verkningsfull informationssäkring ska garantera lämpliga nivåer för konfidentialitet, riktighet, tillgänglighet, oavvislighet och autenticitet. Informationssäkring ska grunda sig 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. Denna bilaga ska tillämpas på alla kommunikations- och informationssystem vid utrikestjänsten som hanterar säkerhetsskyddsklassificerade EU-uppgifter.
3. Kommunikations- och informationssystem ska hantera säkerhetsskyddsklassificerade EU-uppgifter i enlighet med informationssäkringsbegreppet.
4. Alla kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska genomgå en ackrediteringsprocess. Ackrediteringen ska syfta till att skapa förvisning 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 ackrediteringen ska fastställas högsta säkerhetsskyddsklassificeringsnivå för den information som får hanteras av ett system och motsvarande villkor.
5. System som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre ska skyddas på sådant sätt att uppgifterna inte kan läcka ut genom oavsiktlig elektromagnetisk strålning (tempest-säkerhetsåtgärder).
6. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter ska sådana produkter godkännas i enlighet med artikel 8.5 i detta beslut.

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

8. I enlighet med artikel 8.6 i detta beslut kommer följande funktioner för informationssäkring att inrättas i den utsträckning som krävs:

- a) En myndighet för informationssäkring.
- b) En tempestmyndighet.
- c) Den kryptogodkännande myndigheten
- d) Kryptodistribueringsmyndigheten

9. I enlighet med artikel 8.7 i detta beslut ska det för varje system inrättas

- a) en ackrediteringsmyndighet för säkerhet
- b) en driftsansvarig myndighet för informationssäkring.

10. Genomförandebestämmelser för denna artikel anges i bilaga A IV.

Artikel 9

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. Som allmän regel ska sådana kontrakt inte omfatta tillgång till uppgifter som klassificeras TRES SECRET UE/EU TOP SECRET.

2. Utrikestjänsten får genom kontrakt anförtro arbetsuppgifter som omfattar eller medför tillgång till eller hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter till industrienheter eller andra enheter som är registrerade i en medlemsstat, eller i en tredjestat med vilken ett informationssäkerhetsavtal eller en administrativ överenskommelse enligt artikel 10.1 i bilaga A har ingåtts.

3. Utrikestjänsten 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 eller andra enheter tilldelas kontrakt som kräver säkerhetsskyddsavtal. Den ska se till att sådana miniminormer följs i den berörda nationella säkerhetsmyndigheten/utsedda säkerhetsmyndigheten.

4. Entreprenörer eller underentreprenörer som är registrerade i en medlemsstat och som deltar i säkerhetsskyddsklassificerade kontrakt eller underkontrakt som kräver att de hanterar och förvarar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i sina lokaler, antingen när de genomför sådana kontrakt eller innan kontraktet ingås, ska innehålla ett personalsäkerhetsgodkännande av verksamhetsställe på motsvarande säkerhetsskyddsklassificeringsnivå, som utfärdats av den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller en annan behörig säkerhetsmyndighet i den berörda medlemsstaten.

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

6. Genomförandebestämmelser för denna artikel anges i bilaga A V.

Artikel 10

Utbyte av sekretessbelagda uppgifter med tredjestater och internationella organisationer

1. Utrikestjänsten kan endast utbyta säkerhetsskyddsklassificerade EU-uppgifter med en tredjestat eller en internationell organisation om

- a) det finns ett gällande informationssäkerhetsavtal mellan EU och den berörda tredjestaten eller den internationella organisationen, som ingåtts i enlighet med artikel 37 i EU-fördraget och artikel 218 i EUF-fördraget, eller

b) det finns en gällande administrativ överenskommelse mellan den höga representanten och de behöriga säkerhetsmyndigheterna i den tredjestaten eller den internationella organisationen, avseende utbyte av uppgifter som i princip inte har högre säkerhetsskyddsklassificeringsnivå än RESTREINT UE/EU RESTRICTED, som ingåtts i enlighet med det förfarande som anges i artikel 15.5 i detta beslut, eller

c) det finns en tillämplig ram eller ett särskilt avtal om deltagande mellan EU och den berörda tredjestaten inom ramen för GSFP-krishanteringsinsatsen, som ingåtts i enlighet med artikel 37 i EU-fördraget och artikel 218 i EUF-fördraget,

och de villkor som anges i det instrumentet har uppfyllts.

Undantag från huvudregeln ovan anges i bilaga A VI avsnitt V.

2. De administrativa överenskommelser som avses i punkt 1 b 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.

Uppgifter som utbyts på grundval av sådana avtal som avses i punkt 1 c ska begränsas till uppgifter om GSFP-insatser där den berörda tredjestaten deltar på grundval av dessa avtal och i enlighet med bestämmelserna i dessa.

3. Om ett informationssäkerhetsavtal därefter ingås mellan unionen och en bidragande tredjestat eller internationell organisation, ska informationssäkerhetsavtalet ha företräde framför bestämmelsen 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.

4. 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 1–3 och bilaga A VI. 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.

5. Utvärderingsbesök i tredjestater eller internationella organisationer, enligt vad som avses i artikel 17 i detta beslut ska anordnas för att utvärdera säkerhetsåtgärdernas ändamålsenlighet när det gäller att skydda eventuella säkerhetsskyddsklassificerade EU-uppgifter som utbyts.

6. Beslutet att lämna ut säkerhetsskyddsklassificerade EU-uppgifter som innehas av utrikestjänsten till en tredjestat eller internationell organisation ska fattas i varje enskilt fall beroende på uppgifternas karaktär och innehåll, mottagarens behovenliga behörighet och den fördel som EU vinner därigenom.

Utrikestjänsten ska inhämta skriftligt medgivande från sådana enheter som har lämnat säkerhetsskyddsklassificerade uppgifter som källmaterial för säkerhetsskyddsklassificerade EU-uppgifter som utrikestjänsten har upprättat, för att fastställa att det inte finns några hinder för ett utlämnande.

Om det inte är utrikestjänsten som är upphovsman till de säkerhetsskyddsklassificerade uppgifterna, ska utrikestjänsten först söka ett skriftligt medgivande från upphovsmannen.

Om utrikestjänsten emellertid inte kan fastställa upphovsmannen ska utrikestjänstens säkerhetsmyndighet överta upphovsmannens ansvar efter ett enhälligt positivt yttrande från medlemsstaterna genom deras representanter i utrikestjänstens säkerhetskommitté.

7. Genomförandebestämmelser för denna artikel anges i bilaga A VI.

Artikel 11

Överträdelse av säkerhetsbestämmelserna och röjande av säkerhetsskyddsklassificerade uppgifter

1. Eventuella överträdelse eller misstänkta överträdelse av säkerhetsbestämmelserna, och eventuella röjanden eller misstänkta röjanden av säkerhetsskyddsklassificerade uppgifter ska omedelbart rapporteras till utrikestjänstens direktorat med ansvar för säkerhet, som när så är lämpligt ska informera den berörda medlemsstaten eller andra berörda enheter.

2. Om det är känt eller om det föreligger rimliga skäl att misstänka att säkerhetsskyddsklassificerade uppgifter har röjts eller förlorats, ska utrikestjänstens direktorat med ansvar för säkerhet informera den nationella säkerhetsmyndigheten i den berörda medlemsstaten och vidta alla lämpliga åtgärder i enlighet med tillämpliga lagar och andra författningar för att

- a) säkra bevis,
 - b) se till att personal som inte direkt berörs av brottet utreder ärendet för att fastställa fakta,
 - c) omedelbart underrätta upphovsmannen eller varje annan berörd enhet.
 - d) vidta lämpliga åtgärder för att förhindra ett upprepande,
 - e) bedöma den potentiella skada som åsamkats EU:s eller medlemsstaternas intressen, och
 - f) informera de berörda myndigheterna om det faktiska eller misstänkta röjandets effekter och vilka åtgärder som har vidtagits.
3. Alla anställda som utrikestjänsten ansvarar för och som är ansvariga för en överträdelse av säkerhetsbestämmelserna som anges i detta beslut kan komma att underkastas disciplinära åtgärder enligt tillämpliga bestämmelser och föreskrifter.

Varje person som är ansvarig för röjande eller förlust av säkerhetsskyddsklassificerade uppgifter ska underkastas disciplinära och/eller rättsliga åtgärder enligt tillämpliga lagar, bestämmelser och andra författningar.

4. Medan en undersökning av överträdelsen och/eller röjandet pågår får chefen för utrikestjänstens direktorat med ansvar för säkerhet tillfälligt dra in denna persons tillgång till säkerhetsskyddsklassificerade EU-uppgifter och till Europeiska utrikestjänstens lokaler. Säkerhetsdirektoratet vid kommissionens generaldirektoratet för personal och säkerhet, säkerhetsavdelningen vid rådets generalsekretariat eller den nationella säkerhetsmyndigheten i medlemsstaten/medlemsstaterna, eller andra berörda enheter ska omedelbart underrättas om detta beslut.

BILAGA A I

PERSONALSÄKERHET

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser för artikel 5 i bilaga A. Den anger särskilt de kriterier som utrikestjänsten ska tillämpa för att fastställa huruvida en person med beaktande av vederbörandes lojalitet, tillförlitlighet och pålitlighet kan beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter, och de utredningsförfaranden och administrativa förfaranden som ska tillämpas för detta ändamål.
2. "Personalsäkerhetsgodkännande" för tillgång till säkerhetsskyddsklassificerade EU-uppgifter är en förklaring från en behörig myndighet i en medlemsstat, som görs efter en säkerhetsprövning utförd av de behöriga myndigheterna i en medlemsstat och som garanterar att en person, förutsatt att hans eller hennes behovsenliga behörighet har fastställts, får beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum; sådana personer sägs vara "säkerhetsprövade".
3. "Intyg om personalsäkerhetsgodkännande" är ett intyg som utfärdats av utrikestjänstens säkerhetsmyndighet och som fastställer att en person har genomgått säkerhetsprövning, och upp till vilken säkerhetsskyddsklassificeringsnivå för säkerhetsskyddsklassificerade EU-uppgifter som personen kan beviljas tillgång, giltighetstiden för det relevanta personalsäkerhetsgodkännandet samt den dag när själva intyget löper ut.
4. "Tillstånd att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter" är ett tillstånd av utrikestjänstens säkerhetsmyndighet som beviljas i enlighet med detta beslut efter det att ett personalsäkerhetsgodkännande har utfärdats av de behöriga myndigheterna i en medlemsstat, och som intygar att en person, förutsatt att hans eller hennes behovsenliga behörighet har fastställts, beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum; sådana personer sägs vara "säkerhetsprövade".

II. BEVILJANDE AV TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

5. Tillgång till säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED kräver inte någon säkerhetsprövning och beviljas efter det att
 - a) personens rättsliga eller avtalsmässiga koppling till utrikestjänsten har fastställts,
 - b) personens behovsenliga behörighet har fastställts,
 - c) personen har informerats om säkerhetsbestämmelserna och säkerhetsförfarandena för att skydda säkerhetsskyddsklassificerade EU-uppgifter och skriftligen bekräftat sitt ansvar att skydda säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut.
6. En person får endast beviljas tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre efter det att
 - a) personens rättsliga eller avtalsmässiga koppling till utrikestjänsten har fastställts,
 - b) personens behovsenliga behörighet har fastställts,
 - c) personen har fått personalsäkerhetsgodkännande för respektive nivå eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar, och
 - d) personen har informerats om säkerhetsbestämmelserna och säkerhetsförfarandena för att skydda säkerhetsskyddsklassificerade EU-uppgifter och skriftligen bekräftat sitt ansvar i fråga om skyddet av sådana uppgifter.
7. Utrikestjänsten ska fastställa de befattningar i dess strukturer för vilka det krävs tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre och för vilka det därför krävs ett personalsäkerhetsgodkännande upp till den berörda nivån, i enlighet med artikel 4 ovan.
8. Utrikestjänstens personal ska ange om de är medborgare i mer än ett land.

Förfaranden vid utrike tjänsten för begäran om personalsäkerhetsgodkännande

9. För utrike tjänstens personal ska utrike tjänstens tillsättningsmyndighet 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.
10. När en person är medborgare i mer än ett land ska begäran om prövning ställas till den nationella säkerhetsmyndigheten i det land under vars medborgarskap personen har rekryterats.
11. När utrike tjänsten får kännedom om information som är relevant för en säkerhetsprövning och som avser en person som har ansökt om ett personalsäkerhetsgodkännande, ska den i enlighet med tillämpliga bestämmelser och föreskrifter meddela berörd nationell säkerhetsmyndighet detta.
12. När säkerhetsprövningen har slutförts ska den berörda nationella säkerhetsmyndigheten meddela utrike tjänstens direktorat med ansvar för säkerhet resultatet av en sådan prövning.
 - a) När säkerhetsprövningen leder fram till bedömningen att ingenting negativt är känt som skulle kunna ifrågasätta personens lojalitet, tillförlitlighet och pålitlighet, får utrike tjänstens säkerhetsmyndighet bevilja personen i fråga tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till respektive säkerhetsskyddsklassificeringsnivå till och med ett angivet datum.
 - b) Utrike tjänsten ska vidta alla lämpliga åtgärder för att se till att villkor eller begränsningar som införts av de nationella säkerhetsmyndigheterna genomförs på vederbörligt sätt. Den nationella säkerhetsmyndigheten kommer att underrättas om resultatet.
 - c) När säkerhetsprövningen inte leder fram till en sådan positiv bedömning ska utrike tjänstens säkerhetsmyndighet meddela den berörda personen, som kan begära att bli hörd av utrike tjänstens säkerhetsmyndighet. Utrike tjänstens säkerhetsmyndighet får anhålla hos den behöriga nationella säkerhetsmyndigheten om eventuella ytterligare förtydliganden som enligt nationella lagar och andra författningar kan lämnas. Om resultatet bekräftas ska tillgång till säkerhetsskyddsklassificerade EU-uppgifter inte beviljas. I så fall ska utrike tjänsten vidta alla lämpliga åtgärder för att säkerställa att den sökande nekas tillgång till säkerhetsskyddsklassificerade EU-uppgifter.
13. Säkerhetsprövningen och dess resultat, på vilka utrike tjänsten grundar sitt beslut att bevilja eller inte bevilja tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ska omfattas av gällande lagar och andra författningar i den berörda medlemsstaten, inklusive de som gäller överklaganden. Beslut av utrike tjänstens säkerhetsmyndighet ska kunna överklagas i enlighet med tjänsteföreskrifterna.
14. Så länge personalsäkerhetsgodkännandet är giltigt ska de försäkringar på vilka det grundar sig omfatta den berörda personens samtliga uppdrag inom utrike tjänsten, rådets generalsekretariat och kommissionen.
15. Utrike tjänsten ska godta ett eventuellt bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter som beviljats av någon annan av Europeiska unionens institutioner, organ eller byråer, så länge detta fortfarande gäller. Bemyndigandet ska omfatta den berörda personens samtliga uppdrag inom utrike tjänsten. Den unionsinstitution, det unionsorgan eller den unionsbyrå där personen tillträder sin tjänst kommer att meddela relevant nationell säkerhetsmyndighet om bytet av arbetsgivare.
16. Om en persons tjänstgöringsperiod inte påbörjas inom tolv månader från det att utrike tjänstens säkerhetsmyndighet underrättas om resultatet av säkerhetsprövningen, eller om det har skett ett avbrott på 12 månader eller mer i personens tjänstgöring, då vederbörande inte har varit anställda vid utrike tjänsten, vid andra av EU:s institutioner, byråer och organ, eller i en befattning vid en nationell myndighet i en medlemsstat som kräver tillgång till säkerhetsskyddsklassificerade uppgifter, ska detta resultat översändas till den berörda nationella säkerhetsmyndigheten för en bekräftelse av att det fortfarande är giltigt och riktigt.
17. Om utrike tjänsten får kännedom om en säkerhetsrisk som avser en person med giltigt personalsäkerhetsgodkännande, ska den 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. Om en nationell säkerhetsmyndighet meddelar utrike tjänsten att det inte längre finns stöd för den positiva bedömning som gjorts i överensstämmelse med punkt 12 a av en person med ett giltigt tillstånd att tillgå säkerhetsskyddsklassificerade EU-uppgifter får utrike tjänstens säkerhetsmyndighet be den behöriga nationella säkerhetsmyndigheten om ytterligare klargöranden i överensstämmelse med nationella lagar och andra författningar. Om de negativa uppgifterna bekräftas ska ovannämnda tillstånd återkallas och personen ska uteslutas från tillgång till säkerhetsskyddsklassificerade EU-uppgifter och från tjänster där sådan tillgång är möjlig eller där personen i fråga kan äventyra säkerheten.

18. Varje beslut att återkalla ett tillstånd att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter från en person som är anställd vid utrikestjänsten och, när så är lämpligt, skälen till detta, ska meddelas den berörda personen, som kan begära att få höras av utrikestjänstens säkerhetsmyndighet. Information från en nationell säkerhetsmyndighet ska omfattas av gällande relevanta lagar och andra författningar i den berörda medlemsstaten, även i fråga om överklaganden. Beslut av utrikestjänstens säkerhetsmyndighet ska kunna överklagas i enlighet med tjänsteföreskrifterna.
19. Nationella experter som utsänts till utrikestjänsten för befattningar för vilka det krävs tillgång till säkerhetsskyddsklassificerade uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska för utrikestjänstens säkerhetsmyndighet visa upp ett giltigt personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter innan de tillträder sin tjänst. Detta förfarande ska skötas av den utsändande medlemsstaten.

Register över personalsäkerhetsgodkännanden

20. En databas över statusen i fråga om säkerhetsgodkännande för alla anställda som utrikestjänsten ansvarar för och entreprenörer som arbetar för utrikestjänsten ska upprätthållas av Europeiska utrikestjänsten. Dessa register ska omfatta uppgifter om vilken säkerhetsskyddsklassificeringsnivå för säkerhetsskyddsklassificerade EU-uppgifter personen kan få tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), datum för utfärdandet av personalsäkerhetsgodkännandet och dess giltighetstid.
21. Det ska inrättas lämpliga förfaranden för samordning med medlemsstaterna och EU:s institutioner, byråer och organ för att se till att utrikestjänsten har ett korrekt och heltäckande register över statusen i fråga om säkerhetsgodkännande för alla anställda som utrikestjänsten ansvarar för och entreprenörer som arbetar för utrikestjänsten.
22. Utrikestjänstens säkerhetsmyndighet får utfärda ett intyg om personalsäkerhetsgodkännande som visar den nivå på säkerhetsskyddsklassificerade EU-uppgifter som personen kan få tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), giltighetstiden för det relevanta personalsäkerhetsgodkännandet eller tillståndet och det datum intyget löper ut.

Undantag från kravet på personalsäkerhetsgodkännande

23. Personer som vederbörligen beviljats tillgång till säkerhetsskyddsklassificerade EU-uppgifter i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar ska på lämpligt sätt informeras av utrikestjänstens direktorat med ansvar för säkerhet om sina säkerhetsåligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

III. SÄKERHETSUTBILDNING OCH SÄKERHETSMEDEVETENHET

24. Innan de beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska alla personer skriftligen bekräfta att de har förstått sina åligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och följderna av ett röjande av säkerhetsskyddsklassificerade EU-uppgifter. Ett register över sådana skriftliga bekräftelser ska föras av utrikestjänsten.
25. 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.
26. Alla personer som ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska vara föremål för fortlöpande personalsäkerhetsåtgärder (dvs. uppföljning) under den tid de hanterar säkerhetsskyddsklassificerade EU-uppgifter. Ansvar för den kontinuerliga personalsäkerheten åligger följande personer:
 - a) Enskilda personer som beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter: De enskilda personerna är personligen ansvariga för sitt eget uppträdande i säkerhetsfrågor och måste genast till lämpliga säkerhetsmyndigheter rapportera alla beteenden eller aktiviteter som de anser vara misstänkta eller ovanliga, och alla förändringar i deras personliga situation som kan ha en inverkan på personalsäkerhetsgodkännandet eller beviljandet av tillgång till säkerhetsskyddsklassificerade EU-uppgifter.
 - b) Närmast överordnade: De ansvarar för att deras personal är medveten om säkerhetsåtgärderna och ansvarar för att skydda säkerhetsskyddsklassificerade EU-uppgifter, för övervakningen av personalens uppträdande i säkerhetsfrågor och för att antingen själva ta itu med eventuella säkerhetsfrågor eller till berörda säkerhetsmyndigheter rapportera eventuella negativa uppgifter som kan inverka på personalens säkerhetsgodkännande eller tillstånd att få tillgång till sekretessbelagda EU-uppgifter.

- c) Säkerhetsaktörer i utrikestjänstens säkerhetsorganisation som avses i artikel 12 i detta beslut: De ska ansvara för att hålla genomgångar om säkerhetsmedvetenheten för att garantera att personalen inom respektive område får regelbunden information, för att främja en stark säkerhetskultur inom sitt ansvarsområde, för att införa åtgärder för övervakning av personalens uppträdande i säkerhetsfrågor samt för att till berörda säkerhetsmyndigheter rapportera alla negativa uppgifter som kan inverka på enskilda personers personalsäkerhetsgodkännande.
 - d) Utrikestjänsten och medlemsstaterna: De ska införa nödvändiga kanaler för att meddela information som kan inverka på enskilda personers personalsäkerhetsgodkännande eller tillstånd att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter.
27. 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.

IV. SÄRSKILDA OMSTÄNDIGHETER

28. I brådskande fall får utrikestjänstens säkerhetsmyndighet, då detta är välmotiverat 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 inledande kontrollerna för att verifiera att inget negativt framkommit, ge utrikestjänstens tjänstemän och övriga anställda tillfällig behörighet att ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter för en viss funktion. En fullständig säkerhetsprövning bör genomföras så snart som möjligt. Sådana tillfälliga personalsäkerhetstillstånd kommer att vara giltiga under högst sex månader och får inte medge tillgång till information på säkerhetsskyddsklassificeringsnivån TRES 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 utrikestjänsten.
29. När en person ska utnämnas till en tjänst för vilken det krävs ett personalsäkerhetsgodkännande 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 på en högre nivå 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,
 - 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 vid utrikestjänsten,
 - g) den berörda nationella/utsedda säkerhetsmyndighet som utfärdade personens personalsäkerhetsgodkännande har konsulterats och inga invändningar har inkommit, och
 - h) en registrering av undantaget, inklusive en beskrivning av de uppgifter till vilka tillgången beviljades, görs av den enhet som ansvarar för registrering eller dess underenhet.
30. 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 säkerhetsprovats. Detta förfarande får inte upprepas.
31. Under ytterst exceptionella omständigheter, exempelvis tjänsteresor i fientliga miljöer eller under perioder av stigande internationell spänning, får den höga representanten, utrikestjänstens säkerhetsmyndighet eller DGBA 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 personalsäkerhetsgodkännande som krävs, under förutsättning att ett sådant tillstånd är absolut nödvändigt. Detta tillstånd ska registreras med en beskrivning av de uppgifter till vilka tillgång har beviljats.

32. När det gäller uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska denna nödfallstillgång endast beviljas EU-medborgare med behörighet att ha tillgång till antingen den nationella motsvarigheten till uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET eller till SECRET UE/EU SECRET.
33. Utrikestjänstens säkerhetskommitté ska informeras om förfarandet i punkterna 31 och 32 tillämpas.
34. Utrikestjänstens säkerhetskommitté ska få en årlig rapport om användningen av de förfaranden som anges i detta avsnitt.

V. NÄRVARO VID MÖTEN I UTRIKESTJÄNSTENS HÖGKVARTER OCH UNIONENS DELEGATIONER

35. Personer som utsetts att delta i möten i utrikestjänstens högkvarter och unionens delegationer där man diskuterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre får endast göra detta efter det att deras personalsäkerhetsgodkännande har bekräftats. När det gäller medlemsstaternas företrädare samt tjänstemän från rådets generalsekretariat och kommissionen, ska ett intyg om personalsäkerhetsgodkännande eller annat bevis på personalsäkerhetsgodkännande av de behöriga myndigheterna överlämnas till utrikestjänstens direktorat med ansvar för säkerhet eller säkerhetssamordnaren vid unionens delegation eller, i undantagsfall, visas upp av den berörda personen. I tillämpliga fall får en konsoliderad namnförteckning användas där personalsäkerhetsgodkännandet styrks på lämpligt sätt.
36. Om ett personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter återkallas från en person vars arbetsuppgifter kräver närvaro vid möten i utrikestjänstens högkvarter eller unionens delegationer där man diskuterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, ska den behöriga myndigheten underrätta utrikestjänsten om detta.

VI. MÖJLIG TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

37. När personer ska arbeta under omständigheter där de eventuellt kan få tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, ska de genomgå lämplig säkerhetsprövning eller alltid ha ledsagare.
 38. Kurirer, vakter och ledsagare ska säkerhetsprövas upp till den berörda säkerhetsskyddsklassificeringsnivån eller prövas på annat lämpligt sätt i enlighet med nationella lagar och andra författningar samt regelbundet informeras om säkerhetsförfarandena för skydd av säkerhetsskyddsklassificerade EU-uppgifter och om sina åligganden att skydda den information som anförtrotts dem eller som de oavsiktligt kan få tillgång till.
-

BILAGA A II

FYSISK SÄKERHET FÖR SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser för artikel 6 i bilaga A. I bilagan fastställs minimikrav för fysiskt skydd av lokaler, byggnader, kontor, rum och andra utrymmen där säkerhetsskyddsklassificerade EU-uppgifter hanteras och förvaras, inklusive utrymmen som inhyser kommunikations- och informationssystem.
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 behovenlig 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. Utrikestjänsten ska tillämpa ett riskhanteringsförfarande för skydd av säkerhetsskyddsklassificerade EU-uppgifter i sina 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,
 - d) den hotbedömning avseende tredjestater som utarbetats av Europeiska unionens underrättelseanalyscentrum särskilt på grundval av rapporter från unionens delegationer, och
 - e) det bedömda hotet från underrättelsetjänster med EU eller medlemsstaterna som måltavla och det hot som sabotage eller terrorism samt omstörtande eller annan brottslig verksamhet bedöms medföra.
4. Utrikestjänstens säkerhetsmyndighet 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) Inträngsdetekteringssystem: 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) Tillträdeskontroll: 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. and
 - 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. Utrikestjänstens direktorat med ansvar för säkerhet får utföra kontroller vid in- och utpassering för att avskräcka otillåtet införande av material eller otillåtet bortförande 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 utrikestjänstens säkerhetsmyndighet 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 utrikestjänstens säkerhetskommitté.
- 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).
- 13. Utrikestjänstens säkerhetsmyndighet 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 obehörigt tillträde endast beviljas personer som har fått vederbörligt tillstånd av utrikestjänstens direktorat med ansvar för säkerhet, och
 - c) ska övriga personer alltid ledsagas eller genomgå likvärdiga kontroller.
- 15. När det gäller säkrade utrymmen
 - a) ska en synlig yttre gräns upprättas genom vilken alla in- och utpasseringar kontrolleras med hjälp av ett passerkort eller ett system för personigenkänning,

- b) ska obeledsagat tillträde endast beviljas personer som har säkerhetsprövats upp till lämplig nivå och fått särskilt tillstånd att vistas i utrymmet enligt principen om behovsenlig behörighet,
 - c) ska övriga personer alltid ledsagas eller genomgå likvärdiga kontroller.
16. Om 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.
 - c) Elektronisk utrustning ska lämnas utanför detta område.
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 i denna bilaga.
 - 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 utrikestjänstens säkerhetsmyndighet. Sådana inspektioner ska också genomföras efter eventuellt obehörigt intrång eller misstanke om sådant intrång. and
 - d) Utrymmena får inte vara utrustade med otillåtna kommunikationslinjer, otillåtna telefoner eller annan otillåten kommunikationsutrustning och elektrisk eller elektronisk utrustning.
18. Utan hinder av 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 utrikestjänstens säkerhetsmyndighet 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 är installerade.
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) Säkerhetsskyddsklassificeringsnivån på 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 utrikestjänstens säkerhetsmyndighet 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 30–42 i bilaga A III och har åtagit sig att följa de kompensationsåtgärder som anges i säkerhetsföreskrifterna från utrikestjänstens säkerhetsmyndighet 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 utrikestjänstens säkerhetsmyndighet.
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 30–42 i bilaga A III,
 - ii) har åtagit sig att följa de kompensationsåtgärder som anges i säkerhetsanvisningarna från utrikestjänstens säkerhetsmyndighet, 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 den behöriga registreringsenheten detta.
26. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska förvaras i ett säkrat utrymme i ett säkerhetsskåp eller valv.
27. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska hanteras i ett säkrat utrymme.
28. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska förvaras i ett säkrat utrymme vid huvudkvarteret på ett av följande sätt:
- a) I ett säkerhetsskåp som är i överensstämmelse med punkt 8, med en eller flera 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 säkerhetspersonal redo att ingripa om det skulle behövas.
 - b) 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 A III.

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

30. Utrikestjänstens säkerhetsmyndighet 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 skåp,
 - 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 A III

HANTERING AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser för artikel 7 i bilaga A. I bilagan fastställs administrativa åtgärder för att kontrollera säkerhetsskyddsklassificerade EU-uppgifter genom deras hela livscykel för att avskräcka, upptäcka och avhjälpa avsiktligt eller oavsiktligt röjande eller förlust av dessa uppgifter.

II. HANTERING AV SÄKERHETSKLASSNING

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 spridningen av uppgifterna.
4. Säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter ska fastställas i enlighet med artikel 2.2 i bilaga A och genom hänvisning till de säkerhetsriktlinjer som ska godkännas av rådet i enlighet med artikel 3.3 i bilaga A.
5. Säkerhetsskyddsklassificerade uppgifter från medlemsstaterna som utbyts med utrikestjänsten ska tilldelas samma skyddsnivå som säkerhetsskyddsklassificerade EU-uppgifter med motsvarande klassificering. En jämförelsetabell finns i tillägg B till detta beslut.
6. Säkerhetsskyddsklassificeringen och, i förekommande fall, det datum eller den särskilda händelse efter vilken uppgifterna får inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller säkerhetsskyddsklassificeringen hävs, ska anges klart och korrekt, oberoende av huruvida de säkerhetsskyddsklassificerade EU-uppgifterna är i pappersform, muntlig eller elektronisk form, eller i annan form.
7. 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.
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. 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.
10. 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

Märkning

11. Utöver de säkerhetsskyddsklassificeringsnivåer som anges i artikel 2.2 i bilaga A får säkerhetsskyddsklassificerade EU-uppgifter förse med ytterligare markeringar, till exempel följande:
 - a) En markering som anger upphovsman.
 - b) Varningar, 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.

12. Efter ett beslut om att lämna ut säkerhetsskyddsklassificerade EU-uppgifter till en tredjestat eller en internationell organisation ska utrikestjänstens direktorat med ansvar för säkerhet vidarebefordra de berörda säkerhetsskyddsklassificerade uppgifterna, som ska innehålla en markering om att uppgifterna får lämnas ut med angivande av den tredjestat eller internationella organisation till vilken de ska lämnas ut.
13. Utrikestjänstens säkerhetsmyndighet ska anta en förteckning över godkända markeringar.

Förkortade säkerhetsskyddsmarkeringar

14. Standardiserade förkortade säkerhetsskyddsmarkeringar får användas för att ange säkerhetsskyddsklassificeringsnivån för enskilda stycken i en text. Förkortade säkerhetsskyddsmarkeringar får inte ersätta de fullständiga säkerhetsskyddsmarkeringarna.
15. Följande standardförkortningar får användas i säkerhetsskyddsklassificerade EU-handlingar för att ange säkerhetsskyddsklassificeringsnivån för avsnitt eller textstycken vars storlek är mindre än en sida:

TRES 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

16. När en säkerhetsskyddsklassificerad EU-handling upprättas
 - a) ska varje sida tydligt märkas med säkerhetsskyddsklassificeringsnivån,
 - b) ska varje sida numreras,
 - c) ska handlingen förses med ett referensnummer och en ämnesuppgift som inte i sig är en säkerhetsskyddsklassificerad uppgift, om den inte gets en sådan märkning,
 - d) ska handlingen dateras,
 - e) ska handlingar på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ha ett exemplarnummer på varje sida, om de sänds ut i flera exemplar.
17. Om det inte är möjligt att tillämpa punkt 16 på de säkerhetsskyddsklassificerade EU-uppgifterna ska andra lämpliga åtgärder vidtas i enlighet med säkerhetsriktlinjer som ska fastställas i enlighet med detta beslut.

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

18. 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.
19. Utrikestjänsten ska regelbundet se över säkerhetsskyddsklassificerade EU-uppgifter för att förvissa sig om att säkerhetsskyddsklassificeringsnivån fortfarande gäller. Utrikestjänsten ska inrätta ett system för att säkerställa att säkerhetsskyddsklassificeringsnivån för de registrerade säkerhetsskyddsklassificerade EU-uppgifter som det har gett upphov till ses över minst vart femte år. En sådan översyn är inte nödvändig om upphovsmannen redan från början har angett en särskild tidpunkt när uppgifterna automatiskt kommer att inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller när de inte längre behöver vara säkerhetsskyddsklassificerade och uppgifterna har märkts i enlighet med detta.

III. REGISTRERING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER FÖR SÄKERHETSÄNDAMÅL

20. En central registreringsenhet ska inrättas vid huvudkontoret. För varje organisatorisk enhet inom utrikestjänsten där säkerhetsskyddsklassificerade EU-uppgifter hanteras ska det inrättas en ansvarig registreringsenhet, som är underordnad den centrala registreringsenheten, för att garantera att uppgifterna hanteras i enlighet med detta beslut. Registreringsenheterna ska inrättas som säkrade utrymmen enligt definitionen i bilaga A.

Varje unionsdelegation inrättar sin egen registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter.

Utrikestjänstens säkerhetsmyndighet ska utse en chefsregistrator för dessa registreringsenheter.

21. I detta beslut avses med registrering för säkerhetsändamål (nedan kallat *registrering*) tillämpning av förfaranden som registrerar uppgifternas livscykel, inbegripet dess spridning och förstöring. När det gäller ett kommunikations- och informationssystem, får förfarandena utföras genom processer i själva kommunikations- och informationssystemet.
22. Allt material på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre ska registreras när det anländer till eller lämnar en organisatorisk enhet inklusive unionens delegationer. Uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska registreras i de därför avsedda registren.
23. Den centrala registerenheten ska, i utrikestjänstens högkvarter, vara den huvudsakliga kontaktpunkten för in- och utpassering när det gäller utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer. Enheten ska föra ett register över alla dessa utbyten.
24. Utrikestjänstens säkerhetsmyndighet ska godkänna säkerhetsriktlinjer för registrering av säkerhetsskyddsklassificerade EU-uppgifter för säkerhetsändamål, i enlighet med artikel 14 i detta beslut.

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

25. Den centrala registerenheten ska utses i utrikestjänstens huvudkontor och ska fungera som central myndighet för mottagning eller avsändning av uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET. Om det är nödvändigt får underenheter utses för att hantera sådana uppgifter för registreringsändamål.
26. Sådana underenheter får inte överföra handlingar på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET direkt till andra underenheter som är underställda samma centrala registreringsenhet för TRES SECRET UE/EU TOP SECRET eller externt utan uttryckligt godkännande från det senare.

IV. KOPIERING OCH ÖVERSÄTTNING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-HANDLINGAR

27. Handlingar på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET får inte kopieras eller översättas utan föregående skriftligt medgivande från upphovsmannen.
28. 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.
29. De säkerhetsåtgärder som ska tillämpas på originalhandlingarna ska även tillämpas på kopior och översättningar av denna. Kopior av uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska endast skapas av en berörd (under)registreringsenhet med en säker kopieringsmaskin. Kopiorna ska registreras.

V. BEFORDRAN AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

30. Befordran av säkerhetsskyddsklassificerade EU-uppgifter ska omfattas av skyddsåtgärderna i punkterna 32–42. När säkerhetsskyddsklassificerade EU-uppgifter befordras via elektroniska medier, och utan hinder av artikel 7.4 i bilaga A, får skyddsåtgärderna nedan kompletteras med lämpliga tekniska motåtgärder som föreskrivs av utrikestjänstens säkerhetsmyndighet för att minimera risken för att uppgifterna går förlorade eller röjs.
31. Utrikestjänstens säkerhetsmyndighet ska utfärda anvisningar för befordran av säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut.

Inom en byggnad eller ett autonomt byggnadskomplex

32. Säkerhetsskyddsklassificerade EU-uppgifter som befordras inom en byggnad eller ett autonomt byggnadskomplex ska vara övertäckta så att det inte går att se innehållet.
33. Inom en byggnad eller ett autonomt byggnadskomplex ska uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET befordras av vederbörligen säkerhetsprovade personer, i ett förseglat kuvert försett med enbart adressatens namn.

Inom EU

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

35. Befordran av uppgifter på en säkerhetsskyddsklassificeringsnivå upp till SECRET UE/EU SECRET inom EU ska ske med ett av följande medel:
- a) Militär-, regerings- eller diplomatkurir, beroende på vad som är lämpligt.
 - b) Personligt överlämnande förutsatt att
 - i) säkerhetsskyddsklassificerade EU-uppgifter inte lämnas utan uppsikt av budet, såvida de inte förvaras i enlighet med bestämmelserna i bilaga A II,
 - ii) de säkerhetsskyddsklassificerade EU-uppgifterna inte öppnas under befordran eller läses på offentlig plats,
 - iii) personerna har säkerhetsprovats på lämplig nivå och informerats om sina säkerhetsskyldigheter,
 - iv) budet förses med ett kuririntyg när så krävs.
 - c) Posttjänster eller kommersiella kurirtjänster under förutsättning att
 - i) de är godkända av de berörda nationella säkerhetsmyndigheterna enligt nationella lagar och andra författningar,
 - ii) de tillämpar lämpliga skyddsåtgärder enligt de minimikrav som ska fastställas i säkerhetsriktlinjer enligt artikel 21.1 i detta beslut.
- Vid befordran från en medlemsstat till en annan ska bestämmelserna i led c begränsas till att gälla uppgifter på säkerhetsskyddsklassificeringsnivån upp till CONFIDENTIEL UE/EU CONFIDENTIAL.
36. 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 34 ska transporteras såsom frakt av kommersiella transportörer i enlighet med bilaga A V.
37. Fysisk befordran av uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET eller högre mellan byggnader eller lokaler inom EU ska ske med militär-, regerings- eller diplomatkurir, beroende på vad som är lämpligt.

Från EU till en tredjestat eller mellan EU-organ i tredjestater

38. Säkerhetsskyddsklassificerade EU-uppgifter som befordras från EU till en tredjestat, eller mellan EU-organ i tredjestater, ska förpackas så att de skyddas från obehörigt röjande.
39. Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET från EU till en tredjestat, och befordran av alla säkerhetsskyddsklassificerade EU-uppgifter på en säkerhetsskyddsklassificeringsnivå upp till SECRET UE/EU SECRET mellan EU-organ i tredjestater, ska ske med något av följande medel:
- a) Militär- eller diplomatkurir.
 - b) 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 A II,
 - iv) de säkerhetsskyddsklassificerade EU-uppgifterna inte öppnas under befordran eller läses på offentlig plats, och
 - v) personerna har säkerhetsprovats på lämplig nivå och informerats om sina säkerhetsskyldigheter.
40. Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET som EU lämnat till en tredjestat eller internationell organisation ska uppfylla de relevanta bestämmelserna i ett informationssäkerhetsavtal eller en administrativ överenskommelse enligt artikel 10.2 i bilaga A.
41. Säkerhetsskyddsklassificerade uppgifter på nivån RESTREINT UE/EU RESTRICTED får också befordras från EU till en tredjestat med posttjänster eller kommersiella kurirtjänster.

42. Befordran av uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET från EU till en tredjestat eller mellan EU-organ i tredjestater ska ske med militär- eller diplomatkurir.

VI. FÖRSTÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

43. Säkerhetsskyddsklassificerade EU-uppgifter som inte längre behövs får destrueras, utan att det påverkar relevanta bestämmelser om arkivering.
44. Handlingar som är föremål för registrering i enlighet med artikel 7.2 i bilaga A ska destrueras av den ansvariga registreringsenheten enligt innehavarens eller en behörig myndighets anvisningar. Diarier och andra registreringsuppgifter ska uppdateras i enlighet med detta.
45. För handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller TRES 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.
46. 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 TRES 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.
47. Säkerhetsskyddsklassificerade handlingar, inklusive sådana på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, ska destrueras enligt metoder som uppfyller relevant EU-standard eller likvärdiga standarder eller som har godkänts av medlemsstaterna i enlighet med nationella tekniska standarder för att hindra hel eller partiell rekonstruktion.
48. Förstöring av lagringsmedier för datorer som använts för säkerhetsskyddsklassificerade EU-uppgifter ska ske i enlighet med förfaranden som godkänts av utrikestjänstens säkerhetsmyndighet.

VII. SÄKERHETSINSPEKTIONER

Utrikestjänstens säkerhetsinspektioner

49. I enlighet med artikel 16 i detta beslut ska utrikestjänstens säkerhetsinspektioner omfatta följande:
- a) Allmänna säkerhetsinspektioner, vars syfte ska vara att bedöma den allmänna skyddsnivån vid utrikestjänstens högkvarter, unionens delegationer och alla därav beroende eller därmed sammanhängande lokaler, särskilt i syfte att utvärdera effektiviteten hos de säkerhetsåtgärder som genomförs för att skydda utrikestjänstens säkerhetsintressen.
 - b) Säkerhetsinspektioner av säkerhetsskyddsklassificerade EU-uppgifter, vars syfte ska vara att, i allmänhet inför en ackreditering, utvärdera ändamålsenligheten hos de åtgärder som vidtas för att skydda säkerhetsskyddsklassificerade EU-uppgifter i utrikestjänstens högkvarter och unionens delegationer.

Sådana inspektioner ska särskilt genomföras bl.a. för att

- i) garantera att de minimisäkerhetsnormer för skydd av säkerhetsskyddsklassificerade EU-uppgifter som fastställs i detta direktiv respekteras,
- ii) betona vikten av säkerhet och en effektiv riskhantering inom de inspekterade enheterna,
- iii) rekommendera motåtgärder för att minska de specifika konsekvenserna av att de säkerhetsskyddsklassificerade uppgifternas konfidentialitet, riktighet eller tillgänglighet går förlorad, och
- iv) förstärka säkerhetsmyndigheternas fortlöpande program för utbildning och medvetandegörande när det gäller säkerhet.

Genomförande av och rapportering om utrikestjänstens säkerhetsinspektioner

50. Utrikestjänstens säkerhetsinspektioner ska genomföras av en inspektionsgrupp från utrikestjänstens direktorat med ansvar för säkerhet och, vid behov, med stöd av säkerhetsexperter från andra EU-institutioner eller medlemsstaterna.

Inspektionsgruppen ska ha tillträde till alla platser där säkerhetsskyddsklassificerade EU-uppgifter hanteras, särskilt registreringsenheter samt kommunikations- och informationssystemets anslutningspunkter (points of presence).

51. Utrikestjänstens säkerhetsinspektioner i unionens delegationer kan när så är nödvändigt genomföras med stöd av de säkerhetsansvariga vid medlemsstaternas ambassader belägna i de berörda tredjestaterna.
52. Före utgången av varje kalenderår ska utrikestjänstens säkerhetsmyndighet anta ett program för säkerhetsinspektioner för utrikestjänsten för följande år.
53. Säkerhetsinspektioner som inte ingår i programmet kan vid behov anordnas av utrikestjänstens säkerhetsmyndighet.
54. Efter avslutad säkerhetsinspektion ska de viktigaste slutsatserna och rekommendationerna presenteras för den inspekterade enheten. Därefter ska en inspektionsrapport upprättas av inspektionsgruppen. Om korrigerande åtgärder och rekommendationer har föreslagits, ska tillräckligt detaljerade uppgifter för att underbygga de slutsatser som nåtts ingå i rapporten. Rapporten ska överlämnas till utrikestjänstens säkerhetsmyndighet och till chefen för den inspekterade enheten.

En återkommande rapport ska utarbetas under ansvar av utrikestjänstens direktorat med ansvar för säkerhet, i syfte att uppmärksamma de lärdomar som dragits av de inspektioner som genomförts under en angiven tidsperiod och ska granskas av utrikestjänstens säkerhetskommitté.

Genomförande av och rapportering om säkerhetsinspektioner i EU-byråer och EU-organ som inrättats enligt avdelning V kapitel 2 i EU-fördraget

55. Utrikestjänstens direktorat med ansvar för säkerhet får vid behov utse experter som ska delta i gemensamma EU-inspektionsgrupper som genomför inspektioner i EU-byråer och EU-organ som inrättats enligt avdelning V kapitel 2 i EU-fördraget.

Utrikestjänstens checklista för säkerhetsinspektioner

56. Utrikestjänstens direktorat med ansvar för säkerhet ska utarbeta och uppdatera en checklista för säkerhetsinspektioner för de punkter som ska kontrolleras under utrikestjänstens säkerhetsinspektioner. Denna checklista ska översändas till utrikestjänstens säkerhetskommitté.
57. Nödvändiga uppgifter för att fylla i checklistan ska framför allt inhämtas under inspektionen från säkerhetsförvaltningen 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 A IV

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

1. Denna bilaga innehåller genomförandebestämmelser för artikel 8 i bilaga A.
2. Följande egenskaper och begrepp för informationssäkring är av största betydelse för säkerheten och för att driften av kommunikations- och informationssystem ska kunna fungera korrekt:

Autenticitet:	Garanti för att uppgifterna är riktiga och härrör från pålitliga 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 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. Utrikestjänstens behöriga myndigheter 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 hanteringen av säkerhetsrisker ska vara att tillämpa en serie säkerhetsåtgärder som ger en tillfredsställande kompromiss mellan användarkrav och kvarstående säkerhetsrisker.
7. De särskilda krav samt den skala och detaljnivå som fastställs av den berörda ackrediteringsmyndigheten för godkännande 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 innebära 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 det att systemet inleds tills det avslutas.

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 ackrediteringsprocessen för att säkerställa att rätt säkerhetsnivå för de genomförda säkerhetsåtgärderna 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. Utrikestjänsten ska samarbeta med rådets generalsekretariat, kommissionen och medlemsstaterna 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 EU.
15. Spridningen och det efterföljande genomförandet av bästa praxis ska bidra till uppnåendet av en likvärdig säkerhetsnivå för de olika system som används av utrikestjänsten och som hanterar säkerhetsskyddsklassificerade EU-uppgifter.

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) *Avskräckande*: 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 och tillämpliga dessa säkerhetsåtgärder ska vara ska bestämmas genom en riskbedömning.

17. Utrikestjänstens behöriga myndigheter ska se till att de kan bemöta incidenter som kan gå utöver organisatoriska och nationella gränser för att samordna motåtgärder och utbyta information om dessa incidenter och riskerna i samband med dessa (kapacitet för incidenthantering).

Principen om minimalitet och begränsad behörighet

18. Endast 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 efter 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 ackrediteringsprocessen.

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 känna till
 - a) att säkerhetskaverier kan förorsaka betydande skada i systemet och hela organisationen,
 - 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 garantera 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 utrikestjänstens kryptogodkännande myndighet i enlighet med artikel 8.5 i detta beslut 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.
27. När det är motiverat av särskilda operativa skäl får utrikestjänstens kryptogodkännande myndighet på rekommendation av rådets säkerhetskommitté medge undantag från kraven i punkt 25 eller 26 och bevilja interimsgodkännande för en viss period i enlighet med artikel 8.5 i detta beslut.
28. 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.
29. Den höga representanten ska godkänna en säkerhetsstrategi för kvalificering och godkännande av sådana produkter för it-säkerhet som inte används för kryptering.

Överföring inom säkrade områden

30. När överföringen av säkerhetsskyddsklassificerade EU-uppgifter är begränsad till säkrade områden, får trots bestämmelserna i detta beslut okrypterad distribution 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

31. I detta beslut 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.
32. Alla it-system som sammankopplats ska inledningsvis behandlas som icke-tillförlitliga och skyddsåtgärder ska införas för att kontrollera utbytet av säkerhetsskyddsklassificerade uppgifter.
33. 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 ackrediteringsprocess och tillstånd krävs från den behöriga ackrediteringsmyndigheten för säkerhet.
 - c) Gränsskyddstjänster ska genomföras vid den yttre säkerhetsgränsen för samtliga system.
34. Det får inte förekomma sammankoppling 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 sådana sammankopplingar 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 8.5 i detta beslut ska en sådan förbindelse inte betraktas som en sammankoppling.

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

Lagringsmedier för datorer

36. Lagringsmedier för datorer ska destrueras med hjälp av förfaranden som godkänts av utrikestjänstens säkerhetsmyndighet.
37. Lagringsmedier för datorer ska återanvändas, inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller inte längre vara säkerhetsskyddsklassificerade i enlighet med riktlinjer som ska fastställas enligt artikel 8.2 i detta beslut.

Nödlägen

38. Utan hinder av bestämmelserna i detta beslut får de särskilda förfaranden som beskrivs nedan tillämpas under en begränsad tid i en nödsituation, exempelvis under en överhängande eller faktisk kris, konflikt, eller krigssituationer eller under exceptionella operativa omständigheter.
39. 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.
40. 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.

41. Om punkt 39 tillämpas, ska därefter en rapport lämnas till utrikestjänstens direktorat med ansvar för säkerhet och vidarebefordras av denna till utrikestjänstens säkerhetskommitté. I rapporten ska åtminstone avsändaren, mottagaren och upphovsmannen för varje säkerhetsskyddsklassificerad EU-uppgift anges.

III. FUNKTIONER OCH MYNDIGHETER FÖR INFORMATIONSSÄKRING

42. Följande funktioner för informationssäkring ska inrättas vid utrikestjänsten. 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

43. Myndigheten för informationssäkring ska ansvara för att
- a) utforma säkerhetsriktlinjer för informationssäkring och övervaka hur ändamålsenliga och relevanta dessa är,
 - b) skydda och förvalta 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 säkerhetsriktlinjer för informationssäkring, och
 - g) se till att det finns tillgång till lämplig sakkunskap vid expertundergruppen för informationssäkringsfrågor vid utrikestjänstens säkerhetskommitté.

Tempestmyndigheten

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

Den kryptogodkännande myndigheten

45. Den kryptogodkännande myndigheten ska ansvara för att kryptoprodukter överensstämmer med gällande krypteringsriktlinjer. Den ska godkänna en kryptoprodukt för att skydda säkerhetsskyddsklassificerade EU-uppgifter upp till en fastställd säkerhetsskyddsklassificeringsnivå i systemets driftsmiljö.

Kryptodistribueringsmyndigheten

46. Kryptodistribueringsmyndigheten 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.

Akrediteringsmyndigheten för säkerhet

47. Akrediteringsmyndigheten för säkerhet för varje system ska ansvara för att
- a) garantera att kommunikations- och informationssystemen överensstämmer med relevanta 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 akrediteringen och de kriterier enligt vilka nytt godkännande kommer att krävas,

- b) upprätta ett förfarande för säkerhetsackreditering i enlighet med relevanta riktlinjer, 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 redovisning av riskhantering och kvarstående risker, redovisning av systemspecifika säkerhetskrav, kontrolldokumentering av genomförandet av säkerhet och säkra driftsmetoder samt säkerställa att detta överensstämmer med utrikestjänstens säkerhetsbestämmelser och säkerhetsriktlinjer,
 - e) kontrollera genomförandet av säkerhetsåtgärder avseende systemen genom att själv genomföra eller stödja säkerhetsutvärderingar, inspektioner och översyner,
 - f) fastställa säkerhetskrav (t.ex. nivåer för personalsäkerhetsgodkännande) 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 sammankoppling av 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.
48. Ackrediteringsmyndigheten för säkerhet vid utrikestjänsten ska ansvara för att ackreditera alla kommunikations- och informationssystem som fungerar inom utrikestjänstens ansvarsområde.

Ackrediteringsnämnden för säkerhet

49. En gemensam ackrediteringsnämnd för säkerhet ska ansvara för ackreditering av system som omfattas av uppdraget från såväl utrikestjänstens som medlemsstaternas ackrediteringsmyndigheter för säkerhet. Den ska bestå av en företrädare för ackrediteringsmyndigheten för säkerhet från varje medlemsstat, och en företrädare för ackrediteringsmyndigheten för säkerhet vid rådets generalsekretariat och kommissionen 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 utrikestjänstens ackrediteringsmyndighet för säkerhet. Nämnden ska besluta med samförstånd mellan företrädare för institutionernas ackrediteringsmyndigheter för säkerhet, medlemsstaterna och andra enheter med noder i kommunikations- och informationssystemet. Den ska regelbundet avlägga rapport om sin verksamhet till utrikestjänstens säkerhetskommitté och underrätta denna om alla redovisningar av ackreditering.

Den driftsansvariga myndigheten för informationssäkring

50. Den driftsansvariga myndigheten för informationssäkring för varje system ska ansvara för att
- a) utveckla säkerhetsdokumentation i linje med säkerhetsriktlinjer, särskilt redovisningen av systemspecifika säkerhetskrav, inbegripet redovisning av kvarstående risker, säkra driftsmetoder och kryptoplanen inom ackrediteringsprocessen 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 tempest-säkerhetsåtgärder och tempest-säkerhetsutrustning 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,
 - h) genomföra och svara för driften av systemspecifika säkerhetsåtgärder.
-

BILAGA A V

INDUSTRISÄKERHET

I. INLEDNING

1. Denna bilaga innehåller genomförandebestämmelser för artikel 9 i bilaga A. I bilagan fastställs allmänna säkerhetsbestämmelser för företag eller andra enheter vid kontraktsförhandlingar och under hela löptiden för av utrikestjänsten tilldelade kontrakt som kräver säkerhetsskyddsavtal.
2. Utrikestjänstens säkerhetsmyndighet ska godkänna industrisäkerhetsriktlinjer 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 säkerhetsskyddsklassificering

3. Före en anbudsinfordran eller tilldelningen av ett kontrakt ska utrikestjänsten 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. Utrikestjänsten ska i detta syfte utarbeta en handbok om säkerhetsklassning, som ska användas när kontraktet genomförs.
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 utrikestjänsten beakta alla relevanta säkerhetsaspekter, inbegripet den säkerhetsskyddsklassificeringsnivån som uppgifternas upphovsman har fastställt och godkänt för användning i kontraktet.
 - b) Den övergripande sekretessgraden för ett kontrakt får inte vara lägre än den högsta klassningen av någon av dess delar.
 - c) Där så är lämpligt ska utrikestjänsten 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 integrerad 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. Utrikestjänstens direktorat med ansvar för säkerhet ska begära att den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten eller en annan behörig säkerhetsmyndighet i den berörda medlemsstaten, i enlighet med nationella lagar och andra författningar, beviljar ett säkerhetsgodkännande av verksamhetsställe som en indikation på att en industrienhet eller annan enhet kan skydda säkerhetsskyddsklassificerade EU-uppgifter med lämplig säkerhetsskyddsklassificeringsnivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) inom sina anläggningar. Entreprenörer, underentreprenörer eller potentiella sådana ska inte ges eller beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter, förrän bevis på säkerhetsgodkännandet av verksamhetsställe har lämnats till utrikestjänsten.
9. I förekommande fall ska utrikestjänsten, 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.
10. Utrikestjänsten i egenskap av upphandlande myndighet 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.
11. Utrikestjänsten i egenskap av upphandlande myndigheten ska begära att den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet som har utfärdat ett säkerhetsgodkännande av verksamhetsställe underrättar kommissionen om eventuella negativa uppgifter som påverkar godkännandet. När det gäller underentreprenader ska den nationella/utsedda säkerhetsmyndigheten eller annan behörig säkerhetsmyndighet informeras i enlighet med detta.
12. Återkallande av ett säkerhetsgodkännande av verksamhetsställe av en behörig nationell säkerhetsmyndighet/utsedd säkerhetsmyndighet eller annan behörig säkerhetsmyndighet ska utgöra tillräcklig grund för att utrikestjänsten, i egenskap av upphandlande myndighet, ska kunna säga upp kontraktet eller utesluta en anbudsgivare från upphandlingsförfarandet.

IV. PERSONALSÄKERHETSGODKÄNNANDE FÖR ENTREPRENÖRERS PERSONAL

13. All personal som arbetar för entreprenörer som behöver ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska ha genomgått lämplig säkerhetsprövning och ha behövsnlig behörighet att tillgå informationen. Även om ett personalsäkerhetsgodkännande inte krävs för tillgång till säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED, ska en behövsnlig behörighet föreligga för sådan tillgång.
14. Ansökningar om personalsäkerhetsgodkännanden för entreprenörers personal ska göras till den nationella/utsedda säkerhetsmyndighet som ansvarar för enheten.
15. Utrikestjänsten ska för entreprenörer som önskar anställa medborgare från tredjestater i befattningar för vilka det krävs tillgång till säkerhetsskyddsklassificerade EU-uppgifter påpeka att det åligger den nationella/utsedda säkerhetsmyndigheten i den medlemsstat där den anställande enheten är belägen och etablerad att avgöra om den enskilda personen kan beviljas tillgång till sådana uppgifter, i enlighet med detta beslut, och att bekräfta att upphovsmännens samtycke måste ha lämnats innan sådan tillgång ges.

V. KONTRAKT OCH UNDERENTREPRENÖRSKONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL

16. När säkerhetsskyddsklassificerade EU-uppgifter lämnas till en anbudsgivare i det förkontraktuella skedet ska anbudsinfordran innehålla en bestämmelse som förpliktigar en anbudsgivare som inte lämnat något anbud eller valts ut att inom en bestämd tid återlämna alla säkerhetsskyddsklassificerade handlingar.
17. När ett kontrakt eller underentreprenörskontrakt som kräver säkerhetsskyddsavtal har tilldelats ska utrikestjänsten, i egenskap av upphandlande myndighet, underrätta entreprenörens eller underentreprenörens nationella/utsedda säkerhetsmyndighet eller annan behörig säkerhetsmyndighet om säkerhetsbestämmelserna i detta kontrakt.
18. När sådana kontrakt sägs upp eller avslutas ska utrikestjänsten, 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.

19. Som en allmän regel ska entreprenören eller underentreprenören vara skyldig att, efter det att kontraktet eller underentreprenörskontraktet som kräver säkerhetsskyddsavtal har sagts upp eller avslutats, återlämna alla säkerhetsskyddsklassificerade EU-uppgifter till den upphandlande myndigheten.
20. Särskilda bestämmelser för förfogandet över säkerhetsskyddsklassificerade EU-uppgifter under fullgörandet av kontraktet eller sedan det sagts upp eller avslutats ska fastställas i säkerhetsskyddsöverenskommelsen.
21. Om entreprenören eller underentreprenören har tillstånd att behålla säkerhetsskyddsklassificerade EU-uppgifter sedan kontraktet har sagts upp eller avslutats, ska miniminormerna i detta beslut fortsätta att uppfyllas och konfidentialiteten för de säkerhetsskyddsklassificerade EU-uppgifterna ska skyddas av entreprenören eller underentreprenören.
22. De villkor på vilka entreprenören får anlita underentreprenörer ska fastställas i anbudsinfordran och i kontraktet.
23. En entreprenör ska inhämta tillstånd från utrikestjänsten, 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 EU.
24. Entreprenören ska vara ansvarig för att se till att all underentreprenad utförs i enlighet med miniminormerna i detta beslut och får inte lämna ut säkerhetsskyddsklassificerade EU-uppgifter till en underentreprenör utan föregående skriftligt medgivande från den upphandlande myndigheten.
25. När det gäller säkerhetsskyddsklassificerade EU-uppgifter som upprättats eller hanterats av entreprenören eller underentreprenören ska upphovsmannens rättigheter utövas av den upphandlande myndigheten.

VI. BESÖK MED ANKNYTNING TILL KONTRAKT SOM KRÄVER SÄKERHETSSKYDDSAVTAL

26. När utrikestjänsten, 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. Detta påverkar inte den rätt de nationella/utsedda säkerhetsmyndigheterna har, inom ramen för särskilda projekt, att enas om ett förfarande genom vilket sådana besök kan anordnas direkt.
27. Alla besökare ska inneha ett lämpligt personalsäkerhetsgodkännande och ha behovsenlig behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter med anknytning till utrikestjänstens kontrakt.
28. Besökare ska enbart ges tillgång till säkerhetsskyddsklassificerade EU-uppgifter som har samband med besökets syfte.

VII. ÖVERFÖRING OCH BEFORDRAN AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

29. Överföringen av säkerhetsskyddsklassificerade EU-uppgifter på elektronisk väg ska omfattas av tillämpliga bestämmelser i artikel 8 i bilaga A och i bilaga A IV.
30. När det gäller befordran av säkerhetsskyddsklassificerade EU-uppgifter ska tillämpliga bestämmelser i bilaga A III gälla, i enlighet med nationella lagar och andra författningar.
31. Följande principer ska gälla vid fastställandet av säkerhetsarrangemangen för transport av säkerhetsskyddsklassificerat material som frakt:
 - a) Säkerheten ska garanteras i alla skeden av transporten, från ursprungsplatsen till slutdestinationen.
 - b) Den skyddsnivå som ska ges en leverans ska vara den högsta säkerhetsskyddsklassificeringsnivån för det material som leveransen innehåller.
 - c) Ett säkerhetsgodkännande av verksamhetsställe på lämplig nivå ska inhämtas för företag som sköter transporten, om det också innebär att säkerhetsskyddsklassificerade uppgifter förvaras i entreprenörens lokaler. Under alla omständigheter ska den personal som sköter leveransen ha genomgått lämplig säkerhetsprövning i enlighet med bilaga A 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 utrikestjänsten, när så är lämpligt i samverkan med de nationella/utsedda säkerhetsmyndigheterna i både den avsändande och den mottagande medlemsstaten eller annan behörig säkerhetsmyndighet som berörs.
- 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 utrikestjänsten eller annan behörig säkerhetsmyndighet i både den avsändande och den mottagande staten.

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

- 32. Säkerhetsskyddsklassificerade EU-uppgifter ska överföras till entreprenörer och underentreprenörer i tredjestater som har ett giltigt säkerhetsavtal med EU i enlighet med de säkerhetsåtgärder som överenskommits mellan utrikestjänsten, i egenskap av upphandlande myndighet, och den nationella/utsedda säkerhetsmyndigheten i den berörda tredjestat där entreprenören är registrerad.

IX. HANTERING OCH FÖRVAR AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER PÅ SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅN RESTREINT UE/EU RESTRICTED

- 33. Tillsammans med den nationella/utsedda säkerhetsmyndigheten ska utrikestjänsten, 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 säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED som krävs enligt kontraktet har vidtagits.
 - 34. I den omfattning som krävs enligt nationella lagar och andra författningar ska utrikestjänsten såsom den upphandlande myndigheten underrätta de nationella/utsedda säkerhetsmyndigheterna eller annan behörig säkerhetsmyndighet om kontrakt och underentreprenörskontrakt som innehåller säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.
 - 35. Det krävs inte något säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande för entreprenörer eller underentreprenörer och deras personal för kontrakt som tilldelas av utrikestjänsten och som innehåller säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.
 - 36. Utrikestjänsten, i egenskap av upphandlande myndighet, ska granska de anbudssvar som inkommit till följd av meddelandena om upphandling och som avser kontrakt som kräver tillgång till säkerhetsskyddsklassificerade uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, utan hinder av de krav på säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande som kan finnas i nationella lagar och andra författningar.
 - 37. De villkor enligt vilka entreprenören får lägga ut kontrakt på underentreprenad ska överensstämma med punkterna 22–24.
 - 38. När ett kontrakt inbegriper hantering av uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED i ett kommunikations- och informationssystem som sköts av en entreprenör, ska utrikestjänsten 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 A VI

**UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER MED TREDJESTATER OCH
INTERNATIONELLA ORGANISATIONER****I. INLEDNING**

1. Denna bilaga innehåller genomförandebestämmelser för artikel 10 i bilaga A.

II. RAMAR SOM GÄLLER FÖR UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

2. Utrikestjänsten får utbyta säkerhetsskyddsklassificerade EU-uppgifter med tredjestater eller internationella organisationer i enlighet med artikel 10.1 i bilaga A.

Följande ska göras för att stödja den höga representanten vid fullgörandet av de skyldigheter som anges i artikel 218 i EUF-fördraget:

- a) De berörda geografiska eller tematiska avdelningarna vid utrikestjänsten ska, i samråd med utrikestjänstens direktorat med ansvar för säkerhet, när så är lämpligt identifiera behovet av ett långsiktigt utbyte av säkerhetsskyddsklassificerade EU-uppgifter med den berörda tredjestaten eller internationella organisationen.
- b) Utrikestjänstens direktorat med ansvar för säkerhet ska, i samråd med den berörda geografiska avdelningen vid utrikestjänsten, när så är lämpligt för den höga representanten lägga fram de utkast till texter som ska läggas fram för rådet i enlighet med artikel 218.3, 218.5 och 218.6 i EUF-fördraget.
- c) Utrikestjänstens direktorat med ansvar för säkerhet ska stödja den höga representanten vid förhandlingar, i samordning med berörda avdelningar i kommissionen och rådets generalsekretariat.
- d) När det gäller avtal eller arrangemang med tredjestater avseende deras deltagande i GSFP-krishanteringsinsatser i enlighet med artikel 10.1 c i bilaga A, ska utrikestjänstens direktorat för krishantering och planering, i samråd med berörda avdelningar vid utrikestjänsten, när så är lämpligt för den höga representanten lägga fram de utkast till texter som ska läggas fram för rådet i enlighet med artikel 218.3, 218.5 och 218.6 i EUF-fördraget, och ska stödja den höga representanten vid förhandlingar i samordning med berörda avdelningar inom utrikestjänsten och rådets generalsekretariat.
3. Om det finns informationssäkerhetsavtal som föreskriver att tekniska genomförandebestämmelser ska överenskommas mellan utrikestjänstens direktorat med ansvar för säkerhet – i samordning med säkerhetsdirektoratet vid generaldirektoratet för personal och säkerhet och säkerhetsavdelningen vid rådets generalsekretariat – och den behöriga säkerhetsmyndigheten i den berörda tredjestaten eller internationella organisationen, ska sådana bestämmelser ta hänsyn till den skyddsnivå som erbjuds genom befintliga säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden i den berörda tredjestaten eller internationella organisationen.
4. Om det finns ett långvarigt behov för utrikestjänsten att utbyta information med en säkerhetsskyddsklassificeringsnivå som i princip inte är högre än RESTREINT UE/EU RESTRICTED med en tredjestat eller internationell organisation, och om det har fastställts att den berörda parten inte har ett tillräckligt utvecklat säkerhetssystem för att det ska vara möjligt att ingå ett informationssäkerhetsavtal, får den höga representanten, efter ett enhälligt positivt yttrande från utrikestjänstens säkerhetskommitté i enlighet med artikel 15.5 i detta beslut, ingå en administrativ överenskommelse med de behöriga säkerhetsmyndigheterna i den berörda tredjestaten eller internationella organisationen.
5. Inga säkerhetsskyddsklassificerade EU-uppgifter får utbytas på elektronisk väg med en tredjestat eller internationell organisation, såvida detta inte uttryckligen föreskrivs i informationssäkerhetsavtalet eller den administrativa överenskommelsen.
6. Inom ramen för en administrativ överenskommelse om utbyte av säkerhetsskyddsklassificerade uppgifter ska utrikestjänsten och den berörda tredjestaten eller internationella organisationen var för sig utse en registreringsenhet som huvudsaklig kontaktpunkt för in- och utpassering när det gäller de säkerhetsskyddsklassificerade uppgifter som parterna utbyter. För utrikestjänsten ska detta vara utrikestjänstens centrala registerenhet.
7. Administrativa överenskommelser ska i princip ha formen av en skriftväxling.

III. UTVÄRDERINGSBESÖK

8. De utvärderingsbesök som avses i artikel 17 i detta beslut ska genomföras i samförstånd med den berörda tredjestaten eller internationella organisationen, och utvärderingen ska avse
- a) det regelverk som ska tillämpas för att skydda säkerhetsskyddsklassificerade uppgifter,
 - b) eventuella specifika särdrag hos den berörda tredjestatens eller internationella organisationens lagar, bestämmelser, politik eller förfaranden på säkerhetsområdet som kan påverka den högsta säkerhetsskyddsklassificeringsnivån på de uppgifter som kan utbytas,
 - c) de säkerhetsåtgärder och säkerhetsförfaranden som för närvarande finns för skydd av säkerhetsskyddsklassificerade uppgifter, och
 - d) förfaranden för säkerhetsprövning motsvarande säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som ska lämnas ut.
9. Inga säkerhetsskyddsklassificerade EU-uppgifter får utbytas innan ett utvärderingsbesök har genomförts och den nivå på vilken säkerhetsskyddsklassificerade uppgifter får utbytas mellan parterna har fastställts, på grundval av likvärdighet hos det skydd som uppgifterna kommer att ges.

Om den höga representanten, i avvaktan på en sådan inspektion, får kännedom om eventuella exceptionella eller tvingande skäl för utbyte av säkerhetsskyddsklassificerade EU-uppgifter ska utrikestjänsten

- a) först söka erhålla upphovsmannens skriftliga medgivande för att fastställa att det inte finns några invändningar mot ett utlämnande,
- b) hänvisa till utrikestjänstens säkerhetsmyndighet, som får besluta om ett utlämnande, förutsatt att ett enhälligt positivt yttrande från medlemsstaterna genom deras representanter i utrikestjänstens säkerhetskommitté har erhållits.

Om utrikestjänsten inte kan fastställa upphovsmannen ska utrikestjänstens säkerhetsmyndighet överta upphovsmannens ansvar efter att ha erhållit ett enhälligt positivt yttrande från utrikestjänstens säkerhetskommitté.

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

10. När ramar föreligger i enlighet med artikel 10.1 i bilaga A för utbyte av säkerhetsskyddsklassificerade uppgifter med en tredjestat eller internationell organisation ska beslutet att lämna ut säkerhetsskyddsklassificerade EU-uppgifter från utrikestjänsten till en tredjestat eller internationell organisation fattas av utrikestjänstens säkerhetsmyndighet, som får delegera sådana tillstånd till högre tjänstemännen vid utrikestjänsten eller andra personer som står under dess överinseende.
11. Om utrikestjänsten inte är upphovsman till de säkerhetsskyddsklassificerade uppgifter som ska lämnas ut och inte heller till källmaterial som dessa uppgifter kan innehålla, ska utrikestjänsten först söka upphovsmannens skriftliga medgivande för att fastställa att det inte finns några invändningar mot ett utlämnande. Om utrikestjänsten inte kan fastställa upphovsmannen ska utrikestjänstens säkerhetsmyndighet överta upphovsmannens ansvar efter ett enhälligt positivt yttrande från medlemsstaterna genom deras representanter i utrikestjänstens säkerhetskommitté.

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

12. Om en av de ramar som avses i artikel 10.1 i bilaga A saknas och om EU:s eller en eller flera av dess medlemsstaters intressen kräver att säkerhetsskyddsklassificerade EU-uppgifter lämnas ut av politiska, operativa eller brådskande skäl, får säkerhetsskyddsklassificerade EU-uppgifter undantagsvis lämnas ut till en tredjestat eller internationell organisation sedan följande åtgärder har vidtagits.

Efter att ha kontrollerat att villkoren i punkt 11 ovan är uppfyllda ska utrikestjänstens direktorat med ansvar för säkerhet

- 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,

- b) uppmana utrikestjänstens säkerhetskommitté att, utifrån tillgänglig information, avge ett yttrande om tillförlitligheten i säkerhetsbestämmelserna, säkerhetsstrukturerna och säkerhetsförfarandena i den tredjestat eller internationella organisation dit de säkerhetsskyddsklassificerade EU-uppgifterna ska lämnas ut,
 - c) hänvisa till utrikestjänstens säkerhetsmyndighet, som får besluta om ett utlämnande, förutsatt att ett enhälligt positivt yttrande från medlemsstaterna genom deras representanter i utrikestjänsten säkerhetskommitté har erhållits.
13. Om en av de ramar som avses i artikel 10.1 i bilaga A saknas ska den berörda tredje parten skriftligen förbinda sig att skydda de säkerhetsskyddsklassificerade EU-uppgifterna på lämpligt sätt.
-

Tillägg A

Definitioner

I detta beslut gäller följande definitioner:

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.

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

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

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

fysisk säkerhet: tillämpning av fysiska och tekniska skyddsåtgärder för att avskräcka från obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter – se artikel 6 i bilaga A.

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

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 – se bilaga A V, avsnitt II.

handling: registrerad information, oavsett fysisk form eller egenskaper.

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.

hantering av säkerhetsskyddsklassificerade uppgifter: tillämpning av administrativa åtgärder som avser att kontrollera säkerhetsskyddsklassificerade EU-uppgifter genom hela deras livscykel i syfte att komplettera åtgärder som anges i artiklarna 5, 6 och 8 och därigenom avskräcka, upptäcka och avhjälpa avsiktlig eller oavsiktlig läcka eller förlust av dessa uppgifter. Sådana åtgärder gäller särskilt upprättande, registrering, kopiering, översättning, befordran, hantering, förvaring och förstöring av säkerhetsskyddsklassificerade EU-uppgifter – se artikel 7.1 i bilaga A.

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.

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: 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 – se artikel 9.1 i bilaga A.

informationssäkring: förvisningar på området kommunikations- och informationssystem 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. Ändamålsenlig informationssäkring ska garantera lämpliga nivåer för konfidentialitet, riktighet, tillgänglighet, oavvislighet och autenticitet. Informationssäkringen ska grunda sig på en riskhanteringsprocess – se artikel 8.1 i bilaga A.

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

inplacering på lägre säkerhetsskyddsklassificeringsnivå: sänkning av nivån på säkerhetsklassificeringen.

intyg om personalsäkerhetsgodkännande: ett intyg utfärdat av en behörig myndighet där det fastställs att en person är säkerhetsprövad och innehar ett giltigt personalsäkerhetsgodkännande eller av chefen för direktoratet med ansvar för säkerhet 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.

kommunikations- och informationssystem: 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 – se artikel 8.2 i bilaga A.

kontrakt som kräver säkerhetsskyddsavtal: ett kontrakt som ingås av utrikestjänsten 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.

kryptoprodukter: kryptoalgoritmer, maskinvara för kryptering och programvarumoduler, och produkter, inklusive tillämpningsdetaljer med tillhörande dokumentation och nyckelmateriel.

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

känsliga icke-säkerhetsskyddsklassificerade uppgifter: uppgifter eller material som utrikestjänsten måste skydda på grund av rättsliga förpliktelser som fastställs i fördragen eller i rättsakter som antagits för att genomföra dessa, och/eller på grund av uppgifternas eller materielens känslighet. Känsliga, icke-säkerhetsskyddsklassificerade uppgifter inbegriper, men är inte begränsade till, upplysningar eller materiel som omfattas av tystnadsplikt enligt artikel 339 i EUF-fördraget, uppgifter som omfattas av de intressen som skyddas i artikel 4 i Europaparlamentets och rådets förordning (EG) nr 1049/2001 ⁽¹⁾, jämförd med relevant rättspraxis från Europeiska unionens domstol, samt personuppgifter som omfattas av förordning (EG) nr 45/2001.

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

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

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, när det gäller tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, har säkerhetsprövats för den berörda nivån, eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar, och

som har upplysts om sitt ansvar –: se artikel 5.1 i bilaga A.

personalsäkerhetsgodkännande: avser tillgång till säkerhetsskyddsklassificerade EU-uppgifter och är en förklaring från en behörig myndighet i en medlemsstat, som görs efter en säkerhetsprövning utförd av de behöriga myndigheterna i en medlemsstat och som garanterar att en person, förutsatt att hans eller hennes behovsenliga behörighet har fastställts, får beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum; sådana personer sägs vara "säkerhetsprövade".

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.

— redovisning av systemspecifika säkerhetskrav

— en bindande uppsättning säkerhetsprinciper som ska iaktas och detaljerade säkerhetskrav som ska genomföras, som ligger till grund för processen för certifiering och ackreditering av kommunikations- och informationssystem.

— registrering

tillämpning av förfaranden som registrerar uppgifternas livscykel, inbegripet deras spridning och förstöring – se bilaga A III, punkt 21.

⁽¹⁾ Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

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: handlar om att identifiera hot och sårbarheter och utföra därmed sammanhängande riskanalys, dvs. en analys av sannolikhet och konsekvenser.

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

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

röjande av säkerhetsskyddsklassificerade EU-uppgifter: fullständigt eller partiell utlämnande av säkerhetsskyddsklassificerade EU-uppgifter till obehöriga personer eller enheter – se artikel 9.2.

sammankoppling: i detta beslut 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 flervägs kommunikation – se punkt 31 i bilaga A IV.

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.

säkerhetsanvisningar för program/projekt: en förteckning över säkerhetsförfaranden som tillämpas på ett särskilt program/projekt för att standardisera säkerhetsförfaranden. Den kan bli föremål för översyn under hela program-/projektiden.

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 och att den personal som arbetar där och behöver tillgång till säkerhetsskyddsklassificerade EU-uppgifter har säkerhetsgodkänts på lämpligt sätt och informerats om de säkerhetsskydds krav som gäller för att få tillgång till och skydda säkerhetsskyddsklassificerade EU-uppgifter.

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 nationellt personalsäkerhetsgodkännande eller ett EU-personalsäkerhetsgodkännande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre).

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 – se artikel 2 f.

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 – se bilaga A V, avsnitt II.

säkra driftsmetoder: en beskrivning av hur säkerhetsstrategin ska genomföras, av de driftsmetoder som ska användas och av personalens ansvar.

tempest: utredning, undersökning och kontroll av komprometterande elektromagnetisk strålning och åtgärder för att upphäva denna.

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

tillstånd att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter: ett tillstånd av utrikestjänstens säkerhetsmyndighet som ges i enlighet med detta beslut efter det att ett personalsäkerhetsgodkännande har utfärdats av de behöriga myndigheterna i en medlemsstat, och som intygar att en person, förutsatt att hans eller hennes behovsenliga behörighet har fastställts, beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en viss nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum – se artikel 2 i bilaga A I.

underentreprenörskontrakt som kräver säkerhetsskyddsavtal: ett kontrakt som ingås av utrikestjänstens 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.

upphovsman: EU-institution, EU-byrå eller EU-organ, medlemsstat, tredjestat eller internationell organisation under vilkens behörighet säkerhetsskyddsklassificerade uppgifter har upprättats och/eller införts i EU:s strukturer.

utsedd säkerhetsmyndighet: en myndighet som är ansvarig inför medlemsstatens nationella säkerhetsmyndighet och som ansvarar för att informera industrier eller andra enheter om den nationella strategin i alla frågor rörande industri-säkerhet 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.

överträdelse: en handling eller försummelse av en person och som står i strid med säkerhetsbestämmelserna i detta beslut och/eller de säkerhetsstrategier eller säkerhetsriktlinjer där de åtgärder anges som är nödvändiga för beslutets genomförande.

Tillägg B

Likvärdighet mellan säkerhetsskyddsklassificeringsnivåer

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURATOM TOP SECRET	EURATOM SECRET	EURATOM CONFIDENTIAL	EURATOM RESTRICTED
Belgien	Très Secret (Loi 11.12.1998) Zeet 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 Förk.: (ΑΑΠ)	Απόρρητο Förk.: (ΑΠ)	Εμπιστευτικό Förk.: (ΕΜ)	Περιορισμένης Χρήσης Förk.: (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 Förk.: (ΑΑΠ)	Απόρρητο Förk.: (ΑΠ)	Εμπιστευτικό Förk.: (ΕΜ)	Περιορισμένης Χρήσης Förk.: (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-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederländerna	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES 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 HEMLIIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sverige ⁽⁴⁾	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	Ingen motsvarighet ⁽⁵⁾	UK OFFICIAL – SENSITIVE

⁽¹⁾ Diffusion Restreinte/Beperkte Verspreiding är inte en säkerhetsskyddsmarkering i Belgien. Belgien hanterar och skyddar uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE 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 på ett sätt som inte är mindre strängt än de normer och förfaranden som anges i säkerhetsbestämmelserna för Europeiska unionens råd.

⁽⁴⁾ Sverige: Säkerhetsskyddsmarkeringarna i den övre raden används av försvarsmyndigheter och de i den undre raden av övriga myndigheter.

⁽⁵⁾ Förenade kungariket hanterar och skyddar säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL i enlighet med samma säkerhetskrav som gäller för UK SECRET.

ISSN 1977-1061 (elektronisk utgåva)
ISSN 1725-2504 (pappersutgåva)



Europeiska unionens publikationsbyrå
2985 Luxemburg
LUXEMBURG

SV