KOMMISSIONENS BESLUT (EU, Euratom) 2015/444

av den 13 mars 2015

om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 249,

med beaktande av fördraget om upprättandet av Europeiska atomenergigemenskapen, särskilt artikel 106,

med beaktande av protokoll nr 7 om Europeiska unionens immunitet och privilegier som är fogat till fördragen, särskilt artikel 18, och

av följande skäl:

(1) Kommissionens säkerhetsbestämmelser om skydd av säkerhetskyddsklassificerade EU-uppgifter bör ses över och uppdateras, med hänsyn till den institutionella, organisatoriska, driftsmässiga och tekniska utvecklingen.

(2) Europeiska kommissionen har ingått avtal om säkerhetsfrågor för sina viktigaste verksamhetsställen med Belgiens, Luxemburgs och Italiens regeringar ([1]).

(3) Kommissionen, rådet och Europeiska utrikestjänsten (nedan kallad *utrikestjänsten*) är fast beslutna ett tillämpa likvärdiga säkerhetsnormer för skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

(4) Det är viktigt att Europaparlamentet och andra av EU:s institutioner, byråer, organ eller kontor ansluter sig till de principer, normer och regler för skydd av säkerhetsskyddsklassificerade uppgifter som är nödvändiga för att skydda unionens och medlemsstaternas intressen.

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

(6) Inom kommissionen innebär fysisk säkerhet för att skydda säkerhetsskyddsklassificerade uppgifter tillämpning av fysiska och tekniska skyddsåtgärder som är avsedda att hindra obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

(7) Hanteringen av säkerhetsskyddsklassificerade EU-uppgifter innebär tillämpning av administrativa åtgärder som är avsedda att kontrollera säkerhetsskyddsklassificerade EU-uppgifter genom hela deras livscykel i syfte att komplettera de åtgärder som anges i kapitlen 2, 3 och 5 i detta beslut och därigenom avskräcka, upptäcka och avhjälpa avsiktligt eller oavsiktligt röjande eller förlust av dessa uppgifter. Sådana åtgärder gäller särskilt upprättande, lagring, registrering, kopiering, översättning, inplacering på lägre säkerhetsskyddsklassificeringsnivå, hävande av säkerhetsskyddsklassificering, befordran och förstöring av säkerhetsskyddsklassificerade EU-uppgifter, och kompletterar kommissionens allmänna bestämmelser om dokumenthantering (beslut 2002/47/EG, EKSG, Euratom ([2]) och 2004/563/EG, Euratom ([3])).

([1]) Se överenskommelsen om säkerhet mellan Belgiens regering och Europaparlamentet, rådet, kommissionen, Europeiska ekonomiska och sociala kommittén, Regionkommittén och europeiska investeringsbanken av den 31 december 2004 (*Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité*), säkerhetsavtalet mellan kommissionen och Luxemburgs regering av den 20 januari 2007 (*Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois*) och avtalet mellan Italiens regering och Europeiska atomenergigemenskapen (Euratom) av den 22 juli 1959 (*Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale*).

([2]) Kommissionens beslut 2002/47/EG, EKSG, Euratom av den 23 januari 2002 om ändring av dess arbetsordning (EGT L 21, 24.1.2002, s. 23).

([3]) Kommissionens beslut 2004/563/EG, Euratom av den 7 juli 2004 om ändring av dess arbetsordning (EUT L 251, 27.7.2004, s. 9).

(8) Bestämmelserna i detta beslut påverkar inte tillämpningen av

a) förordning (Euratom) nr 3/ ([1]),

b) Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([2]),

c) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([3]),

d) förordning (EEG, Euratom) nr 354/83 ([4]).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

GRUNDLÄGGANDE PRINCIPER OCH MINIMINORMER

Artikel 1

Definitioner

I detta beslut gäller följande definitioner:

1. *kommissionsavdelning*: kommissionens generaldirektorat eller avdelningar, eller en kommissionsledamots kansli.

2. *kryptoprodukter*: kryptoalgoritmer, maskinvara för kryptering och programvarumoduler, och produkter som innehåller tillämpningsdetaljer med tillhörande dokumentation och nyckelmaterial.

3. *beslut att uppgifter inte längre ska vara säkerhetsskyddsklassificerade*: borttagande av varje säkerhetsskyddsklassificering.

4. *Flernivåförsvar*: tillämpningen av ett spektrum av säkerhetsåtgärder som organiseras som multipla försvarsskikt.

5. *Handling*: registrerad information, oavsett fysisk form eller egenskaper.

6. *inplacering på lägre säkerhetsskyddsklassificeringsnivå*: sänkning av nivån på säkerhetsskyddsklassificeringen.

7. *hantering av säkerhetsskyddsklassificerade EU-uppgifter*: all hantering som säkerhetsskyddsklassificerade EU-uppgifter kan utsättas för under hela sin livscykel; detta omfattar deras upprättande, registrering, behandling, befordran, inplacering på lägre säkerhetsskyddsklassificeringsnivå samt 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.

8. *Innehavare*: vederbörligen bemyndigad person som konstaterats ha behovsenlig behörighet och som förfogar över en säkerhetsskyddsklassificerad EU-uppgift och därmed ansvarar för dess skydd.

9. *Genomförandebestämmelser*: en uppsättning regler eller säkerhetsmeddelanden som antagits i enlighet med kapitel 5 i kommissionens beslut (EU, Euratom) 2015/443 ([5]).

10. *materiel*: varje medium, databärare eller maskin eller utrustning som tillverkats eller håller på att tillverkas.

11. *Upphovsman*: EU-institution, EU-byrå eller EU-organ, medlemsstat, tredjestat eller internationell organisation under vars behörighet säkerhetsskyddsklassificerade uppgifter har upprättats och/eller införts i unionens strukturer.

12. *Lokaler*: fast egendom eller därmed likställd egendom i kommissionens ägo eller besittning.

([1]) Förordning (Euratom) nr 3 av den 31 juli 1958 om genomförandet av artikel 24 i fördraget om upprättandet av Europeiska atomenergigemenskapen (EGT 17, 6.10.1958, s. 406/58).
([2]) 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).
([3]) 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).
([4]) Rådets förordning (EEG, Euratom) nr 354/83 av den 1 februari 1983 om öppnandet för allmänheten av Europeiska ekonomiska gemenskapens och Europeiska atomenergigemenskapens historiska arkiv (EGT L 43, 15.2.1983, s. 1).
([5]) Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (se sidan 41 i detta nummer av EUT).

13. *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.

14. *Tjänsteföreskrifter*: tjänsteföreskrifterna för tjänstemän i Europeiska unionen och anställningsvillkoren för övriga anställda i Europeiska unionen, såsom de fastställs i rådets förordning (EEG, Euratom, EKSG) nr 259/68 ([1]).

15. *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.

16. *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, förfaranden, fysiska förhållanden, organisation eller drift.

Artikel 2

Syfte och tillämpningsområde

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

2. Detta beslut ska tillämpas på alla kommissionens avdelningar och lokaler.

3. Utan hinder av särskilda beteckningar för vissa grupper av anställda, ska detta beslut tillämpas på ledamöterna av kommissionen, kommissionens personal som omfattas av tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i Europeiska gemenskaperna, nationella experter som är utstationerade vid kommissionen (nationella experter), tjänsteleverantörer och deras anställda, praktikanter samt var och en som har tillträde till kommissionens byggnader eller andra tillgångar, eller på uppgifter som hanteras av kommissionen.

4. Bestämmelserna i detta beslut ska inte påverka tillämpningen av beslut 2002/47/EG, EKSG, Euratom eller beslut 2004/563/EG, Euratom.

Artikel 3

Definition av säkerhetsskyddsklassificerade EU-uppgifter, säkerhetsskyddsklassificeringsnivå och säkerhetsskyddsmarkeringar

1. Med säkerhetsskyddsklassificerade EU-uppgifter avses uppgifter eller materiel som placerats på en EU-säkerhetsskyddsklassificeringsnivå och vars obehöriga röjande skulle kunna åsamka Europeiska unionens eller en eller flera av dess medlemsstaters väsentliga intressen olika grader av skada.

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

a) TRES SECRET UE/EU TOP SECRET: uppgifter och materiel 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 materiel 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 materiel 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 materiel 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, som inte är säkerhetsskyddsmarkeringar, utan avsedda att ange vilket verksamhetsområde de avser, fastställa upphovsmannen, begränsa utlämning, begränsa användningen eller ange villkor för utlämnande.

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

Artikel 4

Regler för säkerhetsskyddsklassificeringen

1. Varje kommissionsledamot eller kommissionsavdelning ska se till att säkerhetsskyddsklassificerade EU-uppgifter som ledamoten eller avdelningen har givit upphov till placeras på en lämplig säkerhetsskyddsklassificeringsnivå, tydligt identifieras som säkerhetsskyddsklassificerade uppgifter och endast behåller sin säkerhetsskyddsklassificeringsnivå så länge som krävs.

2. Utan att det påverkar tillämpningen av artikel 26 får säkerhetsskyddsklassificerade EU-uppgifter 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 3.2 ändras eller avlägsnas utan föregående skriftligt medgivande från upphovsmannen.

3. I tillämpliga fall ska genomförandebestämmelser om hantering av säkerhetsskyddsklassificerade EU-uppgifter, inklusive en praktisk handbok om säkerhetsskyddsklassificering, antas i enlighet med artikel 60 nedan.

Artikel 5

Skydd av säkerhetsskyddsklassificerade uppgifter

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

2. En innehavare av säkerhetsskyddsklassificerade EU-uppgifter ska vara ansvarig för att skydda dessa uppgifter på ett sätt som är förenligt med detta beslut och dess tillämpningsföreskrifter, i enlighet med de bestämmelser som anges i kapitel 4 nedan.

3. Om medlemsstaterna för in säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsklassificering i kommissionens strukturer eller nät, ska kommissionen skydda uppgifterna i enlighet med kraven för säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå i enlighet med jämförelsetabellen för säkerhetsskyddsklassificeringsnivåer i bilaga I.

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

Artikel 6

Hantering av säkerhetsrisker

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

2. Beredskapsplaner ska beakta behovet att skydda säkerhetsskyddsklassificerade EU-uppgifter i krislägen för att förhindra obehörig tillgång eller röjande, eller att riktighet eller tillgänglighet går förlorad.

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

Artikel 7

Genomförande av detta beslut

1. Vid behov ska tillämpningsföreskrifter för att komplettera eller understödja detta beslut antas i enlighet med artikel 60 nedan.

2. Kommissionens avdelningar ska vidta alla nödvändiga åtgärder inom sitt ansvarsområde för att säkerställa att detta beslut och relevanta tillämpningsföreskrifter tillämpas i samband med hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter eller andra säkerhetsskyddsklassificerade uppgifter.

3. De säkerhetsåtgärder som vidtas för att genomföra detta beslut ska vara förenliga med kommissionens säkerhetsprinciper enligt artikel 3 i beslut (EU, Euratom) nr 2015/443.

4. Generaldirektören för personal och säkerhet ska inrätta kommissionens säkerhetsmyndighet inom generaldirektoratet för personal och säkerhet. Kommissionens säkerhetsmyndighet ska ha de befogenheter som anges i detta beslut och dess tillämpningsföreskrifter.

5. Inom varje kommissionsavdelning ska den lokalt säkerhetsansvariga som avses i artikel 20 i beslut (EU, Euratom) nr 2015/443 ha följande övergripande ansvar för att skydda säkerhetsskyddsklassificerade EU-uppgifter i enlighet med detta beslut, i nära samarbete med generaldirektoratet för personal och säkerhet:

a) Behandla ansökningar om säkerhetsgodkännande av personal.

b) Bidra till säkerhetsutbildning och genomgångar om säkerhetsmedvetenhet.

c) Utöva tillsyn över avdelningens kontrolltjänsteman för registret.

d) Rapportera om överträdelser av säkerhetsbestämmelserna och röjande av säkerhetsskyddsklassificerade EU-uppgifter.

e) Ansvara för reservnycklar och nedtecknade uppgifter om varje kombination.

f) Utföra andra uppgifter som hör samman med skyddet av säkerhetsskyddsklassificerade EU-uppgifter eller som fastställs i tillämpningsföreskrifter.

Artikel 8

Överträdelse av säkerhetsbestämmelserna och röjande av säkerhetsskyddsklassificerade EU-uppgifter

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

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

3. Överträdelser av säkerhetsbestämmelserna eller misstänkta överträdelser av säkerhetsbestämmelserna ska omedelbart rapporteras till kommissionens säkerhetsmyndighet.

4. Om det är känt eller om det föreligger rimliga skäl att anta att säkerhetsskyddsklassificerade EU-uppgifter har röjts eller förlorats, ska en säkerhetsundersökning genomföras i enlighet med artikel 13 i beslut (EU, Euratom) nr 2015/443.

5. Alla nödvändiga åtgärder ska vidtas för att

a) underrätta upphovsmannen,

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

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

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

e) underrätta lämpliga myndigheter om de vidtagna åtgärderna.

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

KAPITEL 2

PERSONALSÄKERHET

Artikel 9

Definitioner

I detta kapitel gäller följande definitioner:

1. *bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter*: ett beslut som kommissionens säkerhetsmyndighet har fattat på grundval av en positiv bedömning från en behörig myndighet i en medlemsstat om att en kommissionstjänsteman, en annan anställd vid kommissionen eller en nationell expert, under förutsättning att personens behovsenliga behörighet har fastställts och denne har fått vederbörlig information om sitt ansvar, beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till en angiven nivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre) till och med ett angivet datum; sådana personer sägs vara ”säkerhetsbemyndigade”.

2. *Personalsäkerhetsbemyndigade*: tillämpning av åtgärder som ska garantera att tillgång till säkerhetsskyddsklassificerade EU-uppgifter endast beviljas personer som

   a) har behovsenlig behörighet,

   b) i förekommande fall har säkerhetsbemyndigats för relevant säkerhetsskyddsklassificeringsnivå, och

   c) har upplysts om sitt ansvar.

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

4. *intyg om personalsäkerhetsgodkännande*: ett intyg utfärdat av en behörig myndighet där det fastställs att en person är säkerhetsprövad och innehar ett giltigt nationellt personalsäkerhetsgodkännande eller ett säkerhetsbemyndigande som utfärdats av kommissionens säkerhetsmyndighet, vilket visar vilken nivå av säkerhetsskyddsklassificerade EU-uppgifter som personen kan få tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), giltighetsdatum för personalsäkerhetsgodkännandet eller personalsäkerhetsbemyndigandet samt vilket datum själva intyget löper ut.

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

Artikel 10

Grundläggande principer

1. En person får beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter när

1. personens behovsenliga behörighet fastställts,

2. personen har informerats om säkerhetsbestämmelserna om skydd av säkerhetsskyddsklassificerade EU-uppgifter och relevanta normer och riktlinjer samt bekräftat sitt ansvar i fråga om skyddet av sådana uppgifter,

3. för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre vederbörande har säkerhetsbemyndigats för den berörda nivån, eller på annat sätt vederbörligen bemyndigats i kraft av sina arbetsuppgifter i enlighet med nationella lagar och andra författningar.

2. Alla personer som för sina arbetsuppgifter kan behöva ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska säkerhetsbemyndigas för respektive säkerhetsskyddsklassificeringsnivå innan de ges tillgång till sådana säkerhetsskyddsklassificerade EU-uppgifter. Den berörda personen ska ge sitt skriftliga medgivande till att genomgå förfarandet för säkerhetsgodkännande av personal. Underlåtenhet att göra detta innebär att vederbörande inte kan tilldelas en tjänst, funktion eller uppgift som medför att denne får tillgång till information på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

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

4. En persons lojalitet, tillförlitlighet och pålitlighet för säkerhetsgodkännande för tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska fastställas genom en säkerhetsprövning som utförs av de behöriga myndigheterna i en medlemsstat i enlighet med dess lagar och andra författningar.

5. Kommissionens säkerhetsmyndighet ska ensam ansvara för att kontakta nationella säkerhetsmyndigheter eller andra behöriga nationella myndigheter i samband med alla frågor som rör säkerhetsgodkännande. Alla kontakter mellan kommissionen och dess personal och de nationella tillsynsmyndigheterna och andra behöriga myndigheter ska ske via kommissionens säkerhetsmyndighet.

Artikel 11

Förfarande för säkerhetsbemyndigande

1. Varje generaldirektör eller avdelningschef inom kommissionen ska fastställa vilka funktioner inom den egna avdelningen som är av sådan natur att de som utför dessa funktioner behöver ha tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre för att kunna utföra sina uppgifter, och därför måste vara säkerhetsbemyndigade.

2. Så snart det är känt att en person kommer att tillsättas på en tjänst som kräver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre, ska den lokalt säkerhetsansvariga vid den berörda kommissionsavdelningen underrätta kommissionens säkerhetsmyndighet, som i sin tur till personen i fråga ska översända det frågeformulär för säkerhetsgodkännande som utfärdats av den nationella säkerhetsmyndigheten i den medlemsstat i vilken personen var medborgare när han eller hon utsågs till en tjänst vid institutionerna. Den berörda personen ska lämna skriftligt medgivande till att genomgå förfarandet för säkerhetsgodkännande och så snart som möjligt återsända det ifyllda formuläret till kommissionens säkerhetsmyndighet.

3. Kommissionens säkerhetsmyndighet ska vidarebefordra det ifyllda frågeformuläret för säkerhetsgodkännande till den nationella säkerhetsmyndigheten i den medlemsstat i vilken personen var medborgare när han eller hon utsågs till en tjänst vid institutionerna, tillsammans med en begäran om säkerhetsprövning för den nivå för säkerhetsskyddsklassificerade EU-uppgifter som personen kommer behöva ha tillgång till.

4. När kommissionens säkerhetsmyndighet har kännedom om information som är relevant för en säkerhetsprövning och som avser en person som har ansökt om ett säkerhetsgodkännande, ska den i enlighet med tillämpliga regler och föreskrifter meddela behörig nationell säkerhetsmyndighet detta.

5. Efter det att säkerhetsprövningen har slutförts, och så snart som möjligt efter det att kommissionens säkerhetsmyndighet har mottagit underrättelse från den berörda nationella säkerhetsmyndigheten om dess samlade bedömning av vad som framkommit vid säkerhetsprövningen, gäller att kommissionens säkerhetsmyndighet

a) får bevilja bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter för den berörda personen och godkänna tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till den relevanta säkerhetsskyddsklassificeringsnivån till och med ett datum som angetts av henne eller honom, dock högst 5 år, när säkerhetsprövningen resulterar i en försäkran om att ingenting negativt är känt som skulle kunna leda till ett ifrågasättande av personens lojalitet, tillförlitlighet och pålitlighet och

b) ska, när säkerhetsprövningen inte resulterar i en sådan försäkran, i enlighet med tillämpliga regler och föreskrifter underrätta den berörda personen, som kan begära att bli hörd av kommissionens säkerhetsmyndighet, som i sin tur får uppmana den behöriga nationella säkerhetsmyndigheten att lämna eventuella ytterligare förtydliganden som den kan tillhandahålla enligt nationella lagar och andra författningar. Om resultatet av säkerhetsprövningen bekräftas ska bemyndigandet att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter inte utfärdas.

6. Säkerhetsprövningen, och de resultat som framkommit, ska omfattas av gällande relevanta lagar och andra författningar i den berörda medlemsstaten, även i fråga om överklagande. Beslut av kommissionens säkerhetsmyndighet ska kunna överklagas i enlighet med tjänsteföreskrifterna.

7. Kommissionens ska godta ett eventuellt bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter som beviljats av någon annan av unionens institutioner, organ eller byråer, så länge detta fortfarande gäller. Bemyndigandet ska omfatta den berörda personens samtliga uppdrag inom kommissionen. Den unionsinstitution, det unionsorgan eller den unionsbyrå där personen tillträder sin tjänst kommer att meddela relevant nationell säkerhetsmyndighet om bytet av arbetsgivare.

8. Om en persons tjänstgöringstid inte påbörjas inom tolv månader efter det att resultatet av säkerhetsprövningen meddelats kommissionens säkerhetsmyndighet, eller om det uppstår ett avbrott på tolv månader i personens tjänstgöring, och vederbörande under tiden inte har varit anställd av kommissionen eller någon annan av unionens institutioner, organ eller byråer, ska kommissionens säkerhetsmyndighet ta upp saken med den berörda nationella säkerhetsmyndigheten för att få bekräftelse på huruvida säkerhetsprövningen fortfarande är giltig och tillämplig.

9. Om kommissionens säkerhetsmyndighet får kännedom om en säkerhetsrisk som avser en person med en giltig säkerhetsprövning, ska säkerhetsmyndigheten i enlighet med tillämpliga bestämmelser meddela detta till den behöriga nationella säkerhetsmyndigheten.

10. Om en nationell säkerhetsmyndighet meddelar kommissionens säkerhetsmyndighet att det inte längre finns stöd för den positiva bedömning som gjorts i överensstämmelse med punkt 5 a av en person med ett giltigt bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter får kommissionens säkerhetsmyndighet be den behöriga nationella säkerhetsmyndigheten om ytterligare klargöranden i överensstämmelse med nationella lagar och andra författningar. Om de negativa uppgifterna bekräftas av den berörda nationella säkerhetsmyndigheten, ska säkerhetsbemyndigandet återkallas och personen uteslutas från tillgång till säkerhetsskyddsklassificerade EU-uppgifter och från tjänster där sådan tillgång är möjlig eller där personen i fråga kan äventyra säkerheten.

11. Alla beslut om att återkalla eller tillfälligt upphäva bemyndigandet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter för en person som omfattas av detta beslut och, i förekommande fall, skälen till detta, ska meddelas den berörda personen, som kan begära att bli hörd av kommissionens säkerhetsmyndighet. Information från en nationell säkerhetsmyndighet ska omfattas av gällande relevanta lagar och andra författningar i den berörda medlemsstaten. Beslut som fattas av kommissionens säkerhetsmyndighet i detta sammanhang ska kunna överklagas i enlighet med tjänsteföreskrifterna.

12. Kommissionens avdelningar ska se till att nationella experter som utstationeras till dem för en tjänst som kräver tillgång till säkerhetsskyddsklassificerade EU-uppgifter, innan de tillträder denna tjänst, uppvisar ett giltigt personalsäkerhetsgodkännande eller intyg om personalsäkerhetsgodkännande, i enlighet med nationella lagar och andra författningar, för kommissionens säkerhetsmyndighet, som på grundval därav beviljar ett bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter upp till den säkerhetsklassificeringsnivå som motsvarar den som avses i det nationella säkerhetsgodkännandet, som maximalt får gälla så länge som utstationeringen varar.

Tillgång till EUCI för personer som vederbörligen bemyndigats i kraft av sina arbetsuppgifter

13. Kommissionsledamöter som har tillgång till säkerhetsskyddsklassificerade EU-uppgifter i kraft av sina arbetsuppgifter på grundval av fördraget, ska informeras om sina säkerhetsskyldigheter när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

Register över säkerhetsgodkännande och säkerhetsbemyndigande

14. Kommissionens säkerhetsmyndighet ska i enlighet med detta beslut föra register över säkerhetsgodkännanden och säkerhetsbemyndiganden som beviljats för tillgång till säkerhetsskyddsklassificerade EU-uppgifter. Dessa register ska åtminstone omfatta uppgifter om vilken säkerhetsskyddsklassificeringsnivå för EU-uppgifter personen kan få tillgång till, datum för utfärdandet av säkerhetsgodkännandet och dess giltighetstid.

15. Kommissionens säkerhetsmyndighet får utfärda ett intyg om personalsäkerhetsgodkännande som visar vilken nivå för säkerhetsskyddsklassificerade EU-uppgifter som personen kan få tillgång till (CONFIDENTIEL UE/EU CONFIDENTIAL eller högre), giltighetsdatum för relevant bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter samt vilket datum själva intyget löper ut.

Förlängning av säkerhetsbemyndiganden

16. Efter det ursprungliga beviljandet av säkerhetsbemyndiganden och under förutsättning att personen oavbrutet har tjänstgjort vid Europeiska kommissionen eller någon annan av unionens institutioner, organ eller byråer och har ett fortsatt behov av tillgång till säkerhetsskyddsklassificerade EU-uppgifter, ska säkerhetsbemyndigandet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter ses över och eventuellt förlängas i princip vart femte år från och med den dag då resultatet av den senaste säkerhetsundersökning på vilken godkännandet grundades meddelades.

17. Kommissionens säkerhetsmyndighet får förlänga giltighetstiden för det befintliga säkerhetsbemyndigandet med upp till 12 månader, om det inte har inkommit någon negativ information från en nationell säkerhetsmyndighet eller annan behörig nationell myndighet inom en period av två månader från den dag då begäran om förlängning med tillhörande frågeformulär om säkerhetsprövning översändes. Om den berörda säkerhetsmyndigheten eller en annan behörig nationell myndighet vid slutet av denna 12-månadersperiod ännu inte har meddelat kommissionen sin ståndpunkt, ska personen tilldelas uppgifter som inte kräver säkerhetsbemyndigande.

Artikel 12

Genomgångar om säkerhetsbemyndigande

1. Efter att ha deltagit i den genomgång om säkerhetsbemyndigande som anordnats av kommissionens säkerhetsmyndighet, ska alla personer som har beviljats ett säkerhetsbemyndigande skriftligen bekräfta att de känner till sina åligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och följderna av att säkerhetsskyddsklassificerade EU-uppgifter röjs. Ett register över sådana skriftliga bekräftelser ska föras av kommissionens säkerhetsmyndighet.

2. 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 kommissionens säkerhetsmyndighet.

3. 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.

Artikel 13

Tillfälliga säkerhetsbemyndiganden

1. I undantagsfall får kommissionens säkerhetsmyndighet, då detta är välmotiverat, ligger i tjänstens intresse och sker 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 inga relevanta negativa uppgifter har framkommit, bevilja personer tillfälligt bemyndigande för tillgång till säkerhetsskyddsklassificerade EU-uppgifter för en viss funktion, utan att detta påverkar tillämpningen av bestämmelserna om förlängning av säkerhetsgodkännanden. Sådana tillfälliga bemyndiganden för tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska vara giltiga under en sammanhängande period på högst sex månader och får inte medge tillgång till information på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET.

2. Efter att ha blivit informerade i enlighet med artikel 12.1 ska alla personer som har beviljats ett tillfälligt säkerhetsbemyndigande skriftligen bekräfta att de känner till sina åligganden när det gäller skyddet av säkerhetsskyddsklassificerade EU-uppgifter och följderna av att säkerhetsskyddsklassificerade EU-uppgifter röjs. Ett register över sådana skriftliga bekräftelser ska föras av kommissionens säkerhetsmyndighet.

Artikel 14

Närvaro vid säkerhetsskyddsklassificerade möten som organiseras av kommissionen

1. Kommissionsavdelningar som ansvarar för att organisera möten där uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre diskuteras ska, genom sin lokalt säkerhetsansvariga eller genom mötesarrangören, underrätta kommissionens säkerhetsmyndighet i god tid om datum, klockslag och plats för samt deltagarna i sådana möten.

2. Om inte annat följer av bestämmelserna i artikel 11.13 får personer som utsetts att delta i möten som organiseras av kommissionen och vid vilka uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre diskuteras endast göra detta efter bekräftelse av att de erhållit säkerhetsbemyndigande eller säkerhetsgodkännande. Rätt att delta i sådana säkerhetsskyddsklassificerade möten ska nekas för personer för vilka kommissionens säkerhetsmyndighet inte har fått ett intyg om personalsäkerhetsgodkännande eller annat bevis på säkerhetsgodkännande, eller för deltagare från kommissionen som inte redan har ett säkerhetsbemyndigande.

3. Innan ett säkerhetsskyddsklassificerat möte organiseras ska den ansvariga mötesorganisatören eller den lokalt säkerhetsansvariga vid den kommissionsavdelning som organiserar mötet begära att externa deltagare överlämnar ett intyg om personalsäkerhetsgodkännande eller annat bevis på säkerhetsgodkännande till kommissionens säkerhetsmyndighet. Kommissionens säkerhetsmyndighet ska underrätta den lokalt säkerhetsansvariga eller mötesorganisatören om intyg om personalsäkerhetsgodkännande eller annat bevis på personalsäkerhetsgodkännande som mottagits. I tillämpliga fall får en konsoliderad namnförteckning användas där säkerhetsgodkännandet styrks på lämpligt sätt.

4. Om kommissionens säkerhetsmyndighet underrättas av behöriga myndigheter om att ett personalsäkerhetsbemyndigande återkallas för en person vars arbetsuppgifter kräver närvaro vid möten som organiseras av kommissionen, ska kommissionens säkerhetsmyndighet meddela den lokalt säkerhetsansvariga vid den kommissionsavdelning som ansvarar för att organisera mötet.

Artikel 15

Potentiell tillgång till säkerhetsskyddsklassificerade EU-uppgifter

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

KAPITEL 3

FYSISK SÄKERHET SOM SYFTAR TILL ATT SKYDDA SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER

Artikel 16

Grundprinciper

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

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

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

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

c) avskräcker, hindrar och avslöjar otillåtna handlingar, och

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

3. Åtgärder för fysisk säkerhet ska vidtas 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 kapitel 5.

4. Utrymmen där säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre förvaras ska fastställas som säkerhetsutrymmen i enlighet med detta kapitel och ackrediteras av kommissionens myndighet för säkerhetsackreditering.

5. Endast utrustning eller anordningar som godkänts av kommissionens säkerhetsmyndighet ska användas för att skydda säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre.

Artikel 17

Fysiska säkerhetskrav och säkerhetsåtgärder

1. Fysiska säkerhetsåtgärder ska väljas på grundval av en hotbedömning som görs av kommissionens säkerhetsmyndighet, i förekommande fall i samråd med andra avdelningar inom kommissionen, andra EU-institutioner, -byråer och -organ och/eller behöriga myndigheter i medlemsstaterna. Kommissionen 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, och

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

2. Kommissionens säkerhetsmyndighet ska med tillämpning av begreppet flernivåförsvar fastställa en lämplig kombination av fysiska säkerhetsåtgärder som ska tillämpas. För detta ändamål ska kommissionens säkerhetsmyndighet utarbeta minimistandarder, normer och kriterier som fastställs i tillämpningsföreskrifterna.

3. Kommissionens säkerhetsmyndighet ska ha rätt att i avskräckande syfte utföra kontroller vid in- eller utpassering mot otillåtet införande av materiel eller otillåtet bortförande av någon form av säkerhetsskyddsklassificerade EU-uppgifter från utrymmen eller byggnader.

4. När det finns en risk för att utomstående kan se säkerhetsskyddsklassificerade EU-uppgifter, även oavsiktligt, ska berörda kommissionsavdelningar vidta lämpliga åtgärder, såsom de definierats av kommissionens säkerhetsmyndighet, för att motverka denna risk.

5. För nya anläggningar ska de fysiska säkerhetskraven och deras funktionsspecifikationer fastställas i samråd med kommissionens säkerhetsmyndighet i samband med planeringen och utformningen av anläggningarna. För befintliga anläggningar ska de fysiska säkerhetskraven tillämpas i enlighet med de minimistandarder, normer och kriterier som fastställs i tillämpningsföreskrifterna.

Artikel 18

Utrustning för fysiskt skydd av säkerhetsskyddsklassificerade EU-uppgifter

1. Två slag av fysiskt skyddade utrymmen ska skapas för att fysiskt skydda säkerhetsskyddsklassificerade EU-uppgifter, nämligen

a) administrativa utrymmen och

b) säkrade utrymmen (inklusive tekniskt säkrade utrymmen).

2. Kommissionens myndighet för säkerhetsackreditering ska fastställa om ett utrymme uppfyller kraven för att betecknas som administrativt utrymme, säkrat utrymme eller tekniskt säkrat utrymme.

3. När det gäller administrativa utrymmen ska

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

b) obeledsagat tillträde ska endast beviljas personer som har fått vederbörligt tillstånd av kommissionens säkerhetsmyndighet eller en annan behörig myndighet, och

c) övriga personer alltid ledsagas eller genomgå likvärdiga kontroller.

4. När det gäller säkrade utrymmen ska

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

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

c) övriga personer alltid ledsagas eller genomgå likvärdiga kontroller.

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

a) Den högsta säkerhetsskyddsklassificeringsnivån för de 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 erhållit vederbörligt säkerhetsgodkännande, såvida åtgärder inte vidtas för att garantera att ingen tillgång till säkerhetsskyddsklassificerade EU-uppgifter är möjlig.

6. Säkrade utrymmen som skyddas mot avlyssning ska betecknas som tekniskt säkrade utrymmen. Följande ytterligare krav ska 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 handhas i enlighet med artikel 20.

b) Alla personer och all materiel som kommer in i dessa utrymmen ska kontrolleras.

c) Utrymmena ska vara föremål för regelbundna fysiska och/eller tekniska inspektioner av kommissionens säkerhetsmyndighet. Sådana inspektioner ska också genomföras efter eventuellt obehörigt intrång eller misstanke om sådant intrång.

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

7. Trots vad som sägs i punkt 6 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 kommissionens säkerhetsmyndighet, som ska försäkra sig om att inga begripliga uppgifter oavsiktligt eller olagligt kan föras ut från det säkrade utrymmet genom sådan utrustning.

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

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

10. Den lokalt säkerhetsansvariga vid den berörda kommissionsavdelningen ska utarbeta säkra driftsmetoder (SecOPs) för varje säkrat utrymme under dennes ansvar, vilka i enlighet med bestämmelserna i detta beslut och dess tillämpningsföreskrifter anger följande:

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

b) Den övervakning och de skyddsåtgärder som ska upprätthållas.

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

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.

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

Artikel 19

Fysiska skyddsåtgärder för hantering och förvar av säkerhetsskyddsklassificerade EU-uppgifter

1. 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 artikel 31 och har åtagit sig att följa de kompensationsåtgärder som fastställs i tillämpningsföreskrifterna för att garantera att säkerhetsskyddsklassificerade EU-uppgifter skyddas från att obehöriga får tillgång till dem.

2. 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 administrativt eller säkrat utrymme, förutsatt att innehavaren har åtagit sig att följa de kompensationsåtgärder som anges i tillämpningsföreskrifterna.

3. 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 att obehöriga får tillgång till dem, eller

c) utanför ett säkrat eller administrativt utrymme förutsatt att innehavaren

   i) har åtagit sig att vidta kompensationsåtgärder i enlighet med tillämpningsföreskrifterna för att se till att de säkerhetsskyddsklassificerade EU-uppgifterna skyddas från att obehöriga får tillgång till dem,

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

   iii) om dokumenten är i pappersform, har meddelat den behöriga registreringsenheten detta.

4. 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.

5. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska hanteras i ett säkrat utrymme som inrättats och drivs av kommissionens säkerhetsmyndighet, och som har ackrediterats till den säkerhetsnivån av kommissionens myndighet för säkerhetsackreditering.

6. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska förvaras i ett säkrat utrymme som har ackrediterats till den säkerhetsnivån av kommissionens myndighet för säkerhetsackreditering; förvaringen ska ske under på ett av följande sätt:

a) I ett säkerhetsskåp, i enlighet med bestämmelserna i artikel 18, med en eller flera av följande kompletterande kontroller:

   1. Kontinuerligt skydd eller kontroll av personal eller vakthavande personal som erhållit säkerhetsgodkännande.

   2. Ett godkänt system för upptäckt av intrång i kombination med säkerhetspersonal redo att ingripa om det skulle behövas.

   eller

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

Artikel 20

Kontroll av nycklar och kombinationer som används för att skydda säkerhetsskyddsklassificerade EU-uppgifter

1. Förfaranden för hantering av nycklar och kombinationer för kontor, rum, valv och säkerhetsskåp ska fastställas i tillämpningsföreskrifter i enlighet med artikel 60. Dessa förfaranden ska vara avsedda att skydda mot obehörigt tillträde.

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

a) vid mottagande av ett nytt säkerhetsskåp,

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

c) vid röjande eller vid misstanke om detta,

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

e) minst var tolfte månad.

KAPITEL 4

HANTERING AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

Artikel 21

Grundprinciper

1. Alla handlingar som innehåller säkerhetsskyddsklassificerade EU-uppgifter bör hanteras i enlighet med kommissionens policy för dokumenthantering och bör således registreras, klassificeras, bevaras och slutligen elimineras, samplas eller överföras till de historiska arkiven i enlighet med den gemensamma bevarandeförteckningen för kommissionens akter.

2. Uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre ska registreras för säkerhetsändamål innan de lämnas ut och när de tas emot. Uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET ska registreras i de därför avsedda registren.

3. Inom kommissionen ska ett system för registrering av säkerhetsskyddsklassificerade EU-uppgifter inrättas i enlighet med bestämmelserna i artikel 27.

4. Kommissionsavdelningar och kommissionsutrymmen inom vilka säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras ska inspekteras med jämna mellanrum av kommissionens säkerhetsmyndighet.

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

a) Som allmän regel ska säkerhetsskyddsklassificerade EU-uppgifter överföras elektroniskt med kryptoprodukter som godkänts i enlighet med kapitel 5.

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

   i) på elektroniska medier (t.ex. USB-minnen, cd-skivor, hårddiskar) som skyddas med kryptoprodukter som godkänts i enlighet med kapitel 5, eller

   ii) i enlighet med vad som föreskrivs i tillämpningsföreskrifter, i alla övriga fall.

Artikel 22

Säkerhetsskyddsklassificeringsnivåer och säkerhetsskyddsmarkeringar

1. Uppgifter ska säkerhetsskyddsklassificeras när deras konfidentialitet behöver skyddas, i enlighet med artikel 3.1.

2. Den som är upphovsman till säkerhetsskyddsklassificerade EU-uppgifter ska vara ansvarig för fastställandet av uppgifternas säkerhetsskyddsklassificeringsnivå i enlighet med relevanta tillämpningsföreskrifter, standarder och riktlinjer för säkerhetsskyddsklassificering och för den första spridningen av uppgifterna.

3. Säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter ska fastställas i enlighet med artikel 3.2 och relevanta tillämpningsföreskrifter.

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

5. 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 i så fall markeras i enlighet med detta, även när de förvaras i elektronisk form.

6. 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.

7. 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.

8. 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

Artikel 23

Markeringar

Utöver de säkerhetsskyddsklassificeringsnivåer som anges i artikel 3.2 får säkerhetsskyddsklassificerade EU-uppgifter förses med ytterligare markeringar, till exempel följande:

a) En markering som anger upphovsman.

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

c) Markering om att uppgifter får lämnas ut.

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

Artikel 24

Förkortade säkerhetsskyddsmarkeringar

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

2. 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

Artikel 25

Upprättande av säkerhetsskyddsklassificerade EU-handlingar

1. När en säkerhetsskyddsklassificerad EU-handling upprättas ska

a) varje sida tydligt märkas med säkerhetsskyddsklassificeringsnivån,

b) varje sida numreras,

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

d) handlingen dateras,

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

2. Om det inte är möjligt att tillämpa punkt 1 på de säkerhetsskyddsklassificerade EU-uppgifterna ska andra lämpliga åtgärder vidtas i enlighet med tillämpningsföreskrifter.

Artikel 26

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

1. I samband med att de upprättas ska upphovsmannen om möjligt ange huruvida de säkerhetsskyddsklassificerade EU-uppgifterna kan inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller huruvida beslut om att uppgifterna inte längre ska vara säkerhetsskyddsklassificerade kan meddelas vid en viss tidpunkt eller efter en särskild händelse.

2. Varje kommissionsavdelning ska regelbundet se över säkerhetsskyddsklassificerade EU-uppgifter för vilka det åligger upphovsmannen att förvissa sig om att säkerhetsskyddsklassificeringsnivån fortfarande gäller. Ett system för att minst vart femte år se över säkerhetsskyddsklassificeringsnivån för registrerade säkerhetsskyddsklassificerade EU-uppgifter som har sitt ursprung i kommissionen ska fastställas genom tillämpningsföreskrifter. En sådan översyn är inte nödvändig om upphovsmannen redan från början har angett att uppgifterna automatiskt kommer att inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller att beslut om att uppgifterna inte längre behöver vara säkerhetsskyddsklassificerade kommer att meddelas och uppgifterna har märkts i enlighet med detta.

3. Uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED som har sitt ursprung i kommissionen kommer automatiskt att förlora sin säkerhetsskyddsklassificering efter trettio år, i enlighet med förordning (EEG, Euratom) nr 354/83, ändrad genom rådets förordning (EG, Euratom) nr 1700/2003 ([1]).

Artikel 27

Systemet för registrering av säkerhetsskyddsklassificerade EU-uppgifter inom kommissionen

1. Utan att det påverkar tillämpningen av artikel 52.5 ska det, inom varje kommissionsavdelning där säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET, inrättas en lokal registreringsenhet med ansvar för säkerhetsskyddsklassificerade EU-uppgifter för att säkerställa att uppgifterna hanteras i enlighet med detta beslut.

2. Den registreringsenhet som förvaltas av generalsekretariatet ska fungera som kommissionens centrala registreringsenhet med ansvar säkerhetsskyddsklassificerade EU-uppgifter. Den ska fungera som

— lokal registreringsenhet med ansvar för säkerhetsskyddsklassificerade EU-uppgifter,

— registreringsenhet med ansvar för säkerhetsskyddsklassificerade EU-uppgifter för kommissionsledamöters privata kontor, såvida inte dessa har en särskild lokal registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter,

— registreringsenhet med ansvar för säkerhetsskyddsklassificerade EU-uppgifter för generaldirektorat eller avdelningar som inte har någon lokal registreringsenhet,

— huvudsaklig kontaktpunkt för in- och utpassering av alla uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED och upp till SECRET UE/EU SECRET som utbyts mellan kommissionen och dess avdelningar och tredjeländer och internationella organisationer och, när så föreskrivs enligt särskilda arrangemang, andra av unionens institutioner, organ och byråer.

3. Inom kommissionen ska kommissionens säkerhetsmyndighet utse en registreringsenhet som 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 dessa uppgifter för registreringsändamål.

4. Underenheterna 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 den senare.

5. Registreringsenheter för säkerhetsskyddsklassificerade EU-uppgifter ska inrättas som säkrade utrymmen enligt definitionen i kapitel 3, och ackrediteras av kommissionens myndighet för säkerhetsackreditering.

Artikel 28

Kontrolltjänsteman för registreringsenheten

1. Varje registreringsenhet med ansvar för säkerhetsskyddsklassificerade EU-uppgifter ska förvaltas av en kontrolltjänsteman för registreringsenheten.

2. Kontrolltjänstemannen ska ha erhållit vederbörligt säkerhetsgodkännande.

3. Kontrolltjänstemannen ska stå under överinseende av den lokalt säkerhetsansvariga inom respektive avdelning vid kommissionen när det gäller tillämpningen av bestämmelser om hantering av handlingar som innehåller säkerhetsskyddsklassificerade EU-uppgifter och efterlevnaden av relevanta säkerhetsbestämmelser, standarder och riktlinjer.

4. Inom ramen för sin roll att sköta den registreringsenhet för säkerhetsklassificerade EU-uppgifter som den lokalt säkerhetsansvariga har anförtrotts ansvaret för, ska denne åta sig följande övergripande uppgifter i enlighet med detta beslut och relevanta tillämpningsföreskrifter, standarder och riktlinjer:

— Handha verksamhet som avser registrering, bevarande, mångfaldigande, översättning, överföring, avsändande och förstöring av säkerhetsskyddsklassificerade EU-uppgifter eller överföring av sådana uppgifter till de historiska arkiven.

— Regelbundet kontrollera behovet av att bibehålla säkerhetsskyddsklassificeringen av uppgifterna.

— Utföra eventuella andra uppgifter i samband med skyddet av säkerhetsskyddsklassificerade EU-uppgifter som fastställs i tillämpningsföreskrifter.

Artikel 29

Registrering av säkerhetsskyddsklassificerade eu-uppgifter för säkerhetsändamål

1. I detta beslut avses med registrering för säkerhetsändamål (nedan kallat *registrering*) tillämpning av förfaranden som innebär registrering av livscykeln för säkerhetsskyddsklassificerade EU-uppgifter, inbegripet deras spridning.

([1]) Rådets förordning (EG, Euratom) nr 1700/2003 av den 22 september 2003 om ändring av förordning (EEG, Euratom) nr 354/83 om öppnandet för allmänheten av Europeiska ekonomiska gemenskapens och Europeiska atomenergigemenskapens historiska arkiv (EUT L 243, 27.9.2003, s. 1).

2. All information och all materiel på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre ska registreras i de därför avsedda registren när de anländer till eller lämnar en organisatorisk enhet.

3. När säkerhetsskyddsklassificerade EU-uppgifter hanteras eller förvaras med hjälp av ett kommunikations- och informationssystem, får registreringsförfarandena utföras genom processer i själva kommunikations- och informationssystemet.

4. Mer detaljerade bestämmelser om registrering av säkerhetsskyddsklassificerade EU-uppgifter för säkerhetsändamål ska fastställas i tillämpningsföreskrifter.

Artikel 30

Kopiering och översättning av säkerhetsskyddsklassificerade EU-handlingar

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

2. 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.

3. De säkerhetsåtgärder som ska tillämpas på originalhandlingen ska även tillämpas på kopior och översättningar av denna.

Artikel 31

Befordran av säkerhetsskyddsklassificerade eu-uppgifter

1. Säkerhetsskyddsklassificerade EU-uppgifter ska befordras på ett sådant sätt att de skyddas från obehörigt röjande.

2. Befordran av säkerhetsskyddsklassificerade EU-uppgifter ska omfattas av skyddsåtgärder, som ska

— stå i proportion till säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som befordras, och

— vara anpassade till de särskilda förutsättningarna för deras befordran, särskilt med hänsyn till om uppgifterna befordras

  — inom en kommissionsbyggnad eller ett autonomt komplex av kommissionsbyggnader,

  — mellan kommissionsbyggnader som är belägna i samma medlemsstat,

  — inom unionen,

  — från unionen till ett tredjeland, och

  — vara anpassade till uppgifternas natur och form.

3. Dessa skyddsåtgärder ska fastställas i detalj i tillämpningsföreskrifter eller, i fråga om projekt och program som avses i artikel 42, som en integrerad del av säkerhetsanvisningarna för det berörda programmet eller projektet.

4. Tillämpningsföreskrifterna eller säkerhetsanvisningarna ska innehålla bestämmelser som står i proportion till säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifterna när det gäller

— typen av befordran, till exempel personligt överlämnande, befordran per diplomatisk eller militär kurir, befordran med posttjänster eller kommersiella kurirtjänster,

— paketering av uppgifterna,

— tekniska motåtgärder för uppgifter som befordras via elektroniska medier,

— någon annan procedurmässig, fysisk eller elektronisk åtgärd,

— registreringsförfaranden,

— användning av säkerhetsgodkänd personal.

5. När säkerhetsskyddsklassificerade EU-uppgifter befordras via elektroniska medier får de skyddsåtgärder som fastställs i relevanta tillämpningsföreskrifter, oaktat vad som sägs i artikel 21.5, kompletteras med lämpliga tekniska motåtgärder som godkänts av kommissionens säkerhetsmyndighet för att minimera risken för att uppgifterna går förlorade eller röjs.

Artikel 32

Förstöring av säkerhetsskyddsklassificerade EU-uppgifter

1. Säkerhetsskyddsklassificerade EU-handlingar som inte längre behövs får förstöras, under hänsyn tagen till arkivregler och till kommissionens regler och föreskrifter om dokumenthantering och arkivering, särskilt den gemensamma förteckningen för bevarande av kommissionens handlingar.

2. Säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre ska förstöras av kontrolltjänstemannen vid den ansvariga registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter på instruktion från innehavaren eller en behörig myndighet. Kontrolltjänstemannen ska uppdatera diarier och annan registreringsinformation i enlighet med detta.

3. För handlingar på säkerhetsskyddsklassificeringsnivån SECRET UE/EU SECRET eller TRES SECRET UE/EU TOP SECRET ska sådan förstöring utföras av kontrolltjänstemannen i närvaro av ett vittne som har säkerhetsgodkänts för minst den säkerhetsskyddsklassificeringsnivå som anges på handlingen som ska förstöras.

4. Registratorn och vittnet, om den senares närvaro krävs, ska underteckna ett förstöringsintyg som ska arkiveras vid registreringsenheten. Kontrolltjänstemannen vid den ansvariga registreringsenheten för säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET 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.

5. Säkerhetsskyddsklassificerade handlingar, inklusive sådana på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED, ska förstöras enligt metoder som ska fastställas i tillämpningsföreskrifter och som uppfyller relevanta EU-standarder eller likvärdiga standarder.

6. Lagringsmedier för datorer som använts för att lagra säkerhetsskyddsklassificerade EU-uppgifter ska förstöras i enlighet med förfaranden som fastställs i tillämpningsföreskrifter.

Artikel 33

Förstöring av säkerhetsskyddsklassificerade EU-uppgifter i nödsituationer

1. Kommissionsavdelningar som innehar säkerhetsskyddsklassificerade EU-uppgifter ska utarbeta planer på grundval av lokala förhållanden för att skydda säkerhetsskyddsklassificerad EU-materiel vid en kris, inklusive nödvändig förstöring i en nödsituation samt planer för evakuering. De ska utfärda de anvisningar som bedöms nödvändiga för att förhindra att säkerhetsskyddsklassificerade EU-uppgifter faller i händerna på obehöriga.

2. Arrangemangen för att skydda och/eller förstöra materiel med beteckningarna CONFIDENTIEL UE/EU CONFIDENTIAL respektive SECRET UE/EU SECRET vid en kris får under inga omständigheter inverka ogynnsamt på skyddet eller förstöringen av materiel med beteckningen TRÈS SECRET UE/EU TOP SECRET, inklusive krypteringsutrustning, vars behandling ska prioriteras framför alla andra åtgärder.

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

4. Mer detaljerade bestämmelser om förstöring av säkerhetsskyddsklassificerade EU-uppgifter ska fastställas i tillämpningsföreskrifter.

KAPITEL 5

SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER I KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

Artikel 34

Grundläggande principer för informationssäkring

1. Med informationssäkring på området kommunikations- och informationssystem avses säkerställande av att dessa system kommer att skydda den information de hanterar och fungera som de ska när det krävs, under kontroll av behöriga användare.

2. Effektiv informationssäkring ska garantera lämpliga nivåer för följande:

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 säkersälla 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.

3. Informationssäkring ska grundas på en riskhanteringsprocess.

Artikel 35

Definitioner

I detta kapitel gäller följande definitioner:

a) *ackreditering*: formellt tillstånd och godkännande som beviljas ett kommunikations- och informationssystem av myndigheten för säkerhetsackreditering att bearbeta säkerhetsskyddsklassificerade EU-uppgifter i systemets driftsmiljö, efter formellt godkännande och korrekt genomförande av skyddsplanen.

b) *ackrediteringsprocess*: de steg och åtgärder som krävs innan myndigheten för säkerhetsackreditering kan bevilja ackreditering; dessa steg och åtgärder ska anges i en standard för ackrediteringsförfarandet.

c) *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.

d) *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.

e) *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.

f) *riskacceptans*: ett beslut efter riskhanteringen om att godta att en kvarstående risk fortfarande existerar.

g) *riskbedömning*: identifiering av hot och sårbarheter och utförande av en därmed sammanhängande riskanalys, dvs. en analys av sannolikhet och konsekvenser.

h) *riskkommunikation*: utveckling av medvetenheten om risker bland systemanvändargrupper, information till tillståndsmyndigheter om sådana risker och rapportering av dessa risker till driftsmyndigheter.

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

Artikel 36

Kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter

1. Kommunikations- och informationssystem ska hantera säkerhetsskyddsklassificerade EU-uppgifter i enlighet med informationssäkringsbegreppet.

2. För system som hanterar säkerhetsskyddsklassificerade EU-uppgifter innebär efterlevnad av kommissionens säkerhetspolicy för informationssystem, såsom denna beskrivs i kommissionens beslut K(2006) 3602 ([1]), att

a) metoden för planering, utförande, kontroll, handling (*Plan-Do-Check-Act*) ska tillämpas vid genomförandet av säkerhetsstrategin för informationssystem under informationssystemets hela livscykel,

b) säkerhetsbehovet ska fastställas genom en konsekvensanalys,

c) informationssystem och data i dessa ska genomgå en formell klassificering av tillgångar,

([1]) K(2006) 3602 av den 16 augusti 2006 om säkerheten i de IT-system som används av Europeiska kommissionen.

d) alla obligatoriska säkerhetsåtgärder som fastställts genom strategin för säkerhet i informationssystem måste genomföras,

e) en riskhanteringsprocess, bestående av följande åtgärder, ska tillämpas: identifiering av hot och sårbarhet, riskbedömning, riskhantering, riskacceptans och riskkommunikation,

f) en säkerhetsplan, inklusive säkerhetspolicy och säkra driftsmetoder, ska definieras, genomföras, kontrolleras och granskas.

3. All personal som arbetar med utformning, utveckling, testning, drift, förvaltning eller användning av kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska underrätta kommissionens myndighet för säkerhetsackreditering om alla potentiella säkerhetsbrister, incidenter, överträdelser av säkerhetsbestämmelser eller röjanden som kan påverka skyddet av kommunikations- och informationssystemet och/eller säkerhetsskyddsklassificerade EU-uppgifter i systemet.

4. Om de säkerhetsskyddsklassificerade EU-uppgifterna skyddas med hjälp av kryptoprodukter, ska dessa produkter godkännas i enlighet med följande:

a) Företräde ska ges till produkter som har godkänts av rådet eller av rådets generalsekreterare, i egenskap av rådets kryptogodkännande myndighet, på rekommendation av kommissionens grupp av säkerhetsexperter.

b) När det är motiverat av särskilda operativa skäl får kommissionens kryptogodkännande myndighet, på rekommendation av kommissionens grupp av säkerhetsexperter, frångå det krav som anges under a och ge tillfälligt godkännande för en viss period.

5. När säkerhetsskyddsklassificerade EU-uppgifter överförs, behandlas och lagras på elektronisk väg ska godkända kryptoprodukter användas. Trots detta krav får specifika förfaranden i krissituationer eller i specifika tekniska konfigurationer tillämpas efter godkännande av kommissionens kryptogodkännande myndighet.

6. Säkerhetsåtgärder ska genomföras för att skydda system som hanterar uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre mot att uppgifterna komprometteras genom oavsiktliga elektromagnetiska läckor (tempestsäkerhetsåtgärder). Sådana säkerhetsåtgärder ska motsvara spridningsrisken och uppgifternas säkerhetsskyddsklassificeringsnivå.

7. Kommissionens säkerhetsmyndighet ska fungera som följande:

— Myndighet för informationssäkring.

— Myndighet för säkerhetsackreditering.

— Tempestmyndighet.

— Kryptogodkännande myndighet.

— Kryptodistribueringsmyndighet.

8. Kommissionen säkerhetsmyndighet ska för varje system utse den driftsansvariga myndigheten för informationssäkring.

9. Ansvaret för de uppgifter som beskrivs i punkterna 7 och 8 kommer att fastställas i tillämpningsföreskrifter.

Artikel 37

Ackreditering av kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter

1. Alla kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska genomgå ett ackrediteringsförfarande som bygger på principerna om informationssäkring, och vars detaljnivå måste stå i proportion till den skyddsnivå som krävs.

2. Till ackrediteringsförfarandet hör att kommissionens myndighet för säkerhetsackreditering formellt validerar säkerhetsplanen för det berörda kommunikations- och informationssystemet för att säkerställa att

a) den riskhanteringsprocess som avses i artikel 36.2 har genomförts på korrekt sätt,

b) systemägaren medvetet har godtagit eventuellt kvarstående risk, och

c) en tillräckligt hög skyddsnivå för de säkerhetsskyddsklassificerade EU-uppgifterna och systemen har uppnåtts i enlighet med detta beslut.

3. Kommissionens säkerhetsmyndighet ska utfärda ett ackrediteringsutlåtande som fastställer den högsta säkerhetsskyddsklassificeringsnivån för de säkerhetsskyddsklassificerade EU-uppgifter som får hanteras i systemet och motsvarande driftsvillkor. Detta påverkar inte de uppgifter som anförtrotts styrelsen för säkerhetsackreditering enligt artikel 11 i Europaparlamentets och rådets förordning (EU) nr 512/2014 ([1]).

4. En gemensam styrelse för säkerhetsackreditering ska ansvara för ackreditering av kommissionens kommunikations- och informationssystem som involverar flera parter. Den ska bestå av en företrädare för respektive medverkande parts myndighet för säkerhetsackreditering, och ha en företrädare för kommissionens myndighet för säkerhetsackreditering som ordförande.

5. Ackrediteringsförfarandet ska bestå av en rad uppgifter för vars genomförande de medverkande parterna ska ansvara. Ansvaret för att förbereda ackrediteringsakter och ackrediteringsunderlag ska helt och hållet åligga ägaren av det berörda kommunikations- och informationssystemet.

6. Ackrediteringsansvaret ska helt och hållet åligga kommissionens myndighet för säkerhetsackreditering som, när som helst under kommunikation- och informationssystemets livscykel ska ha rätt att

a) kräva att ett ackrediteringsförfarande tillämpas,

b) granska eller inspektera systemet,

c) om driftsvillkoren inte längre är uppfyllda, kräva fastställande och ett effektivt genomförande av en plan för förbättrad säkerhet inom en väldefinierad tidsplan, och kunna återkalla tillståndet att använda kommunikations- och informationssystemet tills driftsvillkoren är uppfyllda igen.

7. Ackrediteringsförfarandet ska fastställas i en standard för ackrediteringsförfarandet för kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter, vilken ska antas i enlighet med artikel 10.3 i kommissionens beslut K(2006) 3602.

Artikel 38

Nödlägen

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

2. 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, och

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

3. Säkerhetsskyddsklassificerade EU-uppgifter som överförs under de omständigheter som anges i punkt 1 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.

4. En rapport ska därefter överlämnas till den behöriga myndigheten och till kommissionen grupp av säkerhetsexperter.

KAPITEL 6

INDUSTRISÄKERHET

Artikel 39

Grundprinciper

1. Med industrisäkerhet avses tillämpningen av åtgärder för att garantera skydd av säkerhetsskyddsklassificerade EU-uppgifter

a) inom ramen för säkerhetsskyddsklassificerade kontrakt, av

   i) anbudssökande eller anbudsgivare under upphandlingsförfarandet,

   ii) entreprenörer eller underentreprenörer under hela löptiden av säkerhetsskyddsklassificerade kontrakt,

([1]) Europaparlamentets och rådets förordning (EU) nr 512/2014 av den 16 april 2014 om ändring av förordning (EU) nr 912/2010 om inrättande av en europeisk sjösäkerhetsbyrå (EUT L 150, 20.5.2014, s. 72).

b) inom ramen för säkerhetsskyddsklassificerade bidragsavtal, av

i) de sökande under förfaranden för tilldelning av bidrag,

ii) mottagare under hela livscykeln för säkerhetsskyddsklassificerade bidragsavtal.

2. Sådana kontrakt eller bidragsavtal ska inte omfatta uppgifter på säkerhetsskyddsklassificeringsnivån TRES SECRET UE/EU TOP SECRET.

3. Om inte något annat anges ska bestämmelserna i detta kapitel avseende säkerhetsskyddsklassificerade kontrakt och entreprenörer som måste underteckna säkerhetsskyddsavtal även gälla med avseende på säkerhetsskyddsklassificerade underleverantörskontrakt eller underleverantörer.

Artikel 40

Definitioner

I detta kapitel gäller följande definitioner:

a) *säkerhetsskyddsklassificerat kontrakt*: ett sådant ramavtal eller avtal som avses i rådets förordning (EG, Euratom) nr 1605/2002 ([1]), och som kommissionen eller någon av dess avdelningar har ingått med en entreprenör om leverans av lös eller fast egendom, utförande av byggentreprenader eller tillhandahållande av tjänster, där genomförandet kräver eller inbegriper upprättande, hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter.

b) *underentreprenörskontrakt som kräver säkerhetsskyddsavtal*: kontrakt som en av kommissionens eller en av kommissionens avdelningars leverantörer ingår med en annan leverantör (dvs. underleverantören) om leverans av lös eller fast egendom, utförande av byggentreprenader eller tillhandahållande av tjänster, där genomförandet kräver eller inbegriper upprättande, hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter,

c) *säkerhetsskyddsklassificerat bidragsavtal*: ett avtal varigenom kommissionen beviljar ett bidrag, i den mening som avses i del I avdelning VI i förordning (EG, Euratom) nr 1605/2002, och vars genomförande kräver eller inbegriper upprättande, hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter.

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

Artikel 41

Förfarande för säkerhetsskyddsklassificerade kontrakt eller bidragsavtal

1. Varje kommissionsavdelning som är upphandlande myndighet ska se till att de minimistandarder för industrisäkerhet som fastställs i detta kapitel blir föremål för hänvisning i eller införlivas med kontraktet, och att de följs när industrienheter och andra enheter tilldelas säkerhetsskyddsklassificerade kontrakt eller bidragsavtal.

2. Vid tillämpningen av punkt 1 ska de behöriga avdelningarna inom kommissionen samråda med generaldirektoratet för personal och säkerhet, särskilt dess direktorat för säkerhet, och se till att standardkontrakt och standardunderleverantörskontrakt respektive standardbidragsavtal omfattar bestämmelser som avspeglar de grundläggande principer och minimistandarder för skydd av säkerhetsskyddsklassificerade EU-uppgifter som leverantörer och underleverantörer respektive mottagare av bidrag inom ramen för bidragsavtal ska följa.

3. Kommissionen ska ha ett nära samarbete med den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig myndighet i den berörda medlemsstaten.

4. När en upphandlande myndighet har för avsikt att inleda ett förfarande för att ingå ett säkerhetsskyddsklassificerat kontrakt eller bidragsavtal, ska den under alla etapper av förfarandet samråda med kommissionens säkerhetsmyndighet om frågor som rör förfarandets säkerhetsskyddsklassificerade natur och inslag.

5. Mallar och standarder för säkerhetsskyddsklassificerade kontrakt och underleverantörskontrakt, säkerhetsskyddsklassificerade bidragsavtal, meddelanden om upphandling, vägledning om under vilka omständigheter säkerhetsgodkännande av verksamhetsställe (*Facility Security Clearance*) krävs, säkerhetsanvisningar för program eller projekt, säkerhetsskyddsöverenskommelser, besök, överföring och befordran av säkerhetsskyddsklassificerade EU-uppgifter inom ramen för säkerhetsskyddsklassificerade kontrakt eller bidragsavtal ska fastställas i tillämpningsföreskrifter för industriell säkerhet, efter samråd med kommissionens grupp av säkerhetsexperter.

([1]) Rådets förordning (EG, Euratom) nr 1605/2002 av den 25 juni 2002 med budgetförordning för Europeiska gemenskapernas allmänna budget (EGT L 248, 16.9.2002, s. 1).

6. Kommissionen får ingå säkerhetsskyddsklassificerade kontrakt eller bidragsavtal som innebär att ekonomiska aktörer som är registrerade i en medlemsstat eller en tredjestat med vilken ett avtal eller ett administrativt arrangemang har ingåtts i enlighet med artikel 7 i detta beslut anförtros uppgifter som involverar eller innebär tillgång till eller hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter.

Artikel 42

Säkerhetsinslag i ett säkerhetsskyddsklassificerat kontrakt eller bidragsavtal

1. Säkerhetsskyddsklassificerade kontrakt eller bidragsavtal ska ha följande säkerhetsrelaterade inslag:

Säkerhetsanvisningar för program eller projekt

a) Säkerhetsanvisningar för program eller projekt: en förteckning över säkerhetsförfaranden som tillämpas på ett särskilt program eller projekt för att standardisera säkerhetsförfaranden. Den kan bli föremål för översyn under hela program- eller projekttiden.

b) Generaldirektoratet för personal och säkerhet ska utarbeta allmänna säkerhetsanvisningar för program eller projekt; de kommissionsavdelningar som ansvarar för program eller projekt som innebär hantering eller lagring av säkerhetsklassificerade EU-uppgifter kan vid behov utarbeta särskilda säkerhetsanvisningar för program eller projekt, som ska bygga på de allmänna säkerhetsanvisningarna.

c) Särskilda säkerhetsanvisningar för program eller projekt ska utarbetas bland annat för program och projekt som kännetecknas av sin stora räckvidd, omfattning eller komplexitet, eller av att ett stort antal entreprenörer, stödmottagare och andra berörda parter och intressenter berörs, och dessa uppvisar stora skillnader sinsemellan, exempelvis när det gäller rättslig ställning. Särskilda säkerhetsanvisningar för program eller projekt ska utarbetas av den eller de kommissionsavdelningar som förvaltar programmet eller projektet i fråga, i nära samarbete med generaldirektoratet för personal och säkerhet.

d) Generaldirektoratet för personal och säkerhet ska överlämna både de allmänna och de särskilda säkerhetsanvisningarna för synpunkter till kommissionens grupp av säkerhetsexperter.

Säkerhetsskyddsöverenskommelse

a) En säkerhetsskyddsöverenskommelse är särskilda kontraktsvillkor, som utfärdas av den upphandlande myndigheten och som utgör en integrerad del av varje säkerhetsskyddsklassificerat kontrakt som ger tillgång upphov till säkerhetsskyddsklassificerade EU-uppgifter, och i vilka säkerhetskraven eller de delar av kontraktet som behöver omfattas av säkerhetsskydd fastställs.

b) De kontraktsspecifika säkerhetskraven ska anges i en säkerhetsskyddsöverenskommelse. Säkerhetsskyddsöverenskommelsen ska när så är lämpligt omfatta handboken om säkerhetsklassificering och utgöra en integrerad del av kontraktet eller bidragsavtalet i fråga.

c) Säkerhetsskyddsöverenskommelsen ska innehålla bestämmelser om att entreprenören eller mottagaren ska uppfylla de minimistandarder som fastställs i detta beslut. Den upphandlande myndigheten ska se till att det av säkerhetsskyddsöverenskommelsen framgår att underlåtenhet att iaktta dessa minimistandarder kan utgöra tillräcklig grund för att häva kontraktet eller bidragsavtalet.

2. Både säkerhetsanvisningarna och säkerhetsöverenskommelsen ska omfatta en handbok om säkerhetsskyddsklassificering som obligatoriskt säkerhetsinslag:

a) En handbok om säkerhetsskyddsklassificering är ett dokument som beskriver de delar av ett program, projekt, kontrakt eller bidragsavtal som är säkerhetsskyddsklassificerade, och anger tillämpliga säkerhetsskyddsklassificeringsnivåer. Handboken om säkerhetsskyddsklassificering får utvidgas under hela program-, projekt-, kontrakts- eller bidragsavtalstiden, och delar av uppgifterna kan placeras på en ny eller lägre säkerhetsskyddsklassificeringsnivå; om det finns en handbok om säkerhetsskyddsklassificering ska denna ingå i säkerhetsskyddsöverenskommelsen.

b) Före ett anbudsförfarande eller tilldelningen av ett kontrakt ska den berörda kommissionsavdelningen, i egenskap av upphandlande myndighet, fastställa säkerhetsskyddsklassificeringsnivån för alla uppgifter som ska lämnas ut till anbudssökande, anbudsgivare och entreprenörer, liksom säkerhetsskyddsklassificeringen för eventuella uppgifter som upprättas av entreprenören. För detta ändamål ska kommissionsavdelningen utarbeta en handbok om säkerhetsskyddsklassificering som ska användas vid genomförandet av kontraktet, i enlighet med detta beslut och dess tillämpningsföreskrifter och efter samråd med kommissionens säkerhetsmyndighet.

c) Följande principer ska gälla för fastställande av säkerhetsskyddsklassificeringsnivån för de olika delarna i ett säkerhetsskyddsklassificerat kontrakt:

i) När handboken om säkerhetsskyddsklassificering utarbetas ska den berörda kommissionsavdelningen, i egenskap av upphandlande myndighet, ta hänsyn till alla relevanta säkerhetsaspekter, inbegripet den säkerhetsskyddsklassificeringsnivå som uppgifternas upphovsman har fastställt och godkänt för användning i kontraktet.

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

iii) Där så är lämpligt ska den upphandlande myndigheten, genom kommissionens säkerhetsmyndighet, 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.

Artikel 43

Tillgång till säkerhetskyddsklassificerade EU-uppgifter för entreprenörers och stödmottagares personal

Den upphandlande eller beviljande myndigheten ska se till att det säkerhetsskyddsklassificerade kontraktet eller bidragsavtalet innehåller bestämmelser om att personal hos entreprenörer, underentreprenörer eller bidragsmottagare som för att kunna genomföra det säkerhetsskyddsklassificerade kontraktet eller bidragsavtalet måste ha tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska beviljas sådan tillgång endast om vederbörande

a) har erhållit säkerhetsbemyndigande på relevant nivå eller på annat sätt är vederbörligen bemyndigad genom sin behovsenliga behörighet,

b) har informerats om tillämpliga säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter och bekräftat sitt ansvar när det gäller att skydda sådana uppgifter,

c) har erhållit säkerhetsgodkännande på en nivå som är relevant för uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET av respektive nationell säkerhetsmyndighet, utsedd säkerhetsmyndighet eller någon annan behörig myndighet.

Artikel 44

Intyg om säkerhetsgodkännande av verksamhetsställe

1. Säkerhetsgodkännande av verksamhetsställe är ett administrativt beslut av en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller någon annan behörig säkerhetsmyndighet om att ett verksamhetsställe ur säkerhetsperspektiv kan erbjuda tillräckligt säkerhetsskydd av säkerhetsskyddsklassificerade EU-uppgifter på en specificerad säkerhetsskyddsklassificeringsnivå.

2. Ett säkerhetsgodkännande av verksamhetsställe som beviljas av den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet i en medlemsstat i syfte att visa, i enlighet med nationella lagar och andra författningar, att en ekonomisk aktör har förmåga att skydda säkerhetsskyddsklassificerade EU-uppgifter på lämplig säkerhetsskyddsklassificeringsnivå (CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET) inom sina anläggningar, ska lämnas till kommissionens säkerhetsmyndighet, som ska vidarebefordra det till den kommissionsavdelning som fungerar som upphandlande eller beviljande myndighet, innan en anbudssökande, anbudsgivare eller entreprenör, eller bidragssökande eller bidragsmottagare får ges eller beviljas tillgång till säkerhetsskyddsklassificerade EU-uppgifter.

3. I förekommande fall ska den upphandlande myndigheten, genom kommissionens säkerhetsmyndighet, underrätta vederbörlig nationell säkerhetsmyndighet, utsedd säkerhetsmyndighet eller någon annan behörig säkerhetsmyndighet att det krävs ett säkerhetsgodkännande av verksamhetsställe för att genomföra kontraktet. Det ska krävas ett säkerhetsgodkännande av verksamhetsställe eller ett personalsäkerhetsgodkännande när säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET måste tillhandahållas under upphandlings- eller bidragstilldelningsförfarandets gång.

4. Den upphandlande eller bidragsbeviljande myndigheten får inte tilldela en vald anbudsgivare eller deltagare ett säkerhetskyddsklassificerat kontrakt eller bidragsavtal innan den har fått bekräftat från den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig myndighet i den medlemsstat där den berörda entreprenören eller underentreprenören är registrerad att ett giltigt intyg om säkerhetsgodkännande av verksamhetsställe har utfärdats, om ett sådant krävs.

5. När kommissionens säkerhetsmyndighet har underrättats av den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller en annan behörig säkerhetsmyndighet som har utfärdat ett säkerhetsgodkännande av verksamhetsställe om eventuella ändringar med avseende på detta godkännande, ska den underrätta den kommissionsavdelning som fungerar som upphandlande eller bidragsbeviljande myndighet. Vid eventuell underentreprenad ska den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet underrättas om detta.

6. Återkallande av ett säkerhetsgodkännande av verksamhetsställe av en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet eller någon annan behörig säkerhetsmyndighet ska utgöra tillräcklig grund för att den upphandlande eller bidragsbeviljande myndigheten ska kunna säga upp kontraktet eller utestänga en anbudssökande, anbudsgivare eller sökande från förfarandet. En bestämmelse om detta ska ingå i de standardkontrakt och standardbidragsavtal som ska utarbetas.

Artikel 45

Bestämmelser om säkerhetsskyddsklassificerade kontrakt och bidragsavtal

1. När säkerhetsskyddsklassificerade EU-uppgifter lämnas till en anbudssökande, en anbudsgivare eller en sökande under ett upphandlingsförfarande, ska inbjudan att lämna anbud eller inbjudan att lämna förslag innehålla en bestämmelse som förpliktigar anbudssökanden, anbudsgivaren eller den sökande som inte inkommer med ett anbud eller ett förslag eller som inte väljs ut att återlämna alla säkerhetsskyddsklassificerade handlingar inom en viss tid.

2. Den upphandlande eller beviljande myndigheten ska, genom kommissionens säkerhetsmyndighet, underrätta den behöriga nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet om att ett säkerhetsskyddsklassificerat kontrakt eller bidragsavtal har tilldelats, och om de uppgifter som berörs, t.ex. namnet på entreprenören (entreprenörerna) eller bidragsmottagaren (bidragsmottagarna) kontraktets löptid och den högsta säkerhetsskyddsklassificeringsnivån.

3. När sådana kontrakt eller bidragsavtal upphör att gälla ska den upphandlande eller beviljande myndigheten omedelbart anmäla detta till kommissionens säkerhetsmyndighet, den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet i den medlemsstat där entreprenören eller bidragsmottagaren är registrerad.

4. Som en allmän regel ska entreprenören eller bidragsmottagaren, när det säkerhetsskyddsklassificerade kontraktet eller bidragsavtalet upphör att gälla eller en bidragsmottagare avslutar sitt deltagande, vara skyldig att återlämna alla säkerhetsskyddsklassificerade EU-uppgifter som innehas av denne.

5. Särskilda bestämmelser för förfogandet över säkerhetsskyddsklassificerade EU-uppgifter under fullgörandet av ett säkerhetsskyddsklassificerat kontrakt eller bidragsavtal eller sedan det upphört att gälla ska fastställas i säkerhetsskyddsöverenskommelsen.

6. Om entreprenören eller bidragsmottagaren har rätt att behålla säkerhetsskyddsklassificerade EU-uppgifter sedan det säkerhetsskyddsklassificerade kontraktet har upphört att gälla, ska minimistandarderna i detta beslut fortsätta att uppfyllas och konfidentialiteten för de säkerhetsskyddsklassificerade EU-uppgifterna ska skyddas av entreprenören eller bidragsmottagaren.

Artikel 46

Särskilda bestämmelser om säkerhetsskyddsklassificerade kontrakt

1. De villkor av relevans för skyddet av säkerhetsskyddsklassificerade EU-uppgifter på vilka entreprenören får anlita underentreprenörer ska fastställas i anbudsinfordran och i det säkerhetsskyddsklassificerade kontraktet.

2. En entreprenör ska inhämta tillstånd från den upphandlande myndigheten, innan delar av kontraktet läggs ut på en underentreprenör. Inga underleverantörsavtal som innebär tillgång till säkerhetsskyddsklassificerade EU-uppgifter får tilldelas underentreprenörer som är registrerade i ett tredjeland, såvida det inte finns ett regelverk om informationssäkerhet i enlighet med kapitel 7.

3. 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.

4. När det gäller säkerhetsskyddsklassificerade EU-uppgifter som upprättats eller hanterats av entreprenören, ska kommissionen anses vara upphovsman, och upphovsmannens rättigheter ska utövas av den upphandlande myndigheten.

Artikel 47

Besök med anknytning till säkerhetsskyddsklassificerade kontrakt

1. När personal vid kommissionen eller hos entreprenörer eller bidragsmottagare begär tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i varandras lokaler för att genomföra ett säkerhetsskyddsklassificerat kontrakt eller bidragsavtal, ska besök anordnas tillsammans med de berörda nationella säkerhetsmyndigheterna, de utsedda säkerhetsmyndigheterna eller andra behöriga säkerhetsmyndigheter. Kommissionens säkerhetsmyndighet ska informeras om sådana besök. När det gäller särskilda program eller projekt får dock de nationella säkerhetsmyndigheterna, de utsedda säkerhetsmyndigheterna eller någon annan behörig säkerhetsmyndighet även enas om ett förfarande varigenom sådana besök kan anordnas direkt.

2. Alla besökare ska inneha ett lämpligt säkerhetsgodkännande och ha behovsenlig behörighet för tillgång till säkerhetsskyddsklassificerade EU-uppgifter med anknytning till det säkerhetsskyddsklassificerade kontraktet.

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

4. Närmare bestämmelser ska fastställas i tillämpningsföreskrifter.

5. Det ska vara obligatoriskt att följa bestämmelserna om besök i samband med säkerhetsskyddsklassificerade kontrakt i detta beslut och i de tillämpningsföreskrifter som avses i punkt 4.

Artikel 48

Översändande och befordran av säkerhetsskyddsklassificerade EU-uppgifter i samband med säkerhetsskyddsklassificerade kontrakt eller bidragsavtal

1. Överföring av säkerhetsskyddsklassificerade EU-uppgifter på elektronisk väg ska omfattas av tillämpliga bestämmelser i kapitel 5 i detta beslut.

2. När det gäller befordran av säkerhetsskyddsklassificerade EU-uppgifter ska tillämpliga bestämmelser i kapitel 4 i detta beslut och i dess tillämpningsföreskrifter gälla, i enlighet med nationella lagar och andra författningar.

3. Följande principer ska gälla vid fastställandet av säkerhetsarrangemangen för transport av säkerhetsskyddsklassificerad materiel 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 den materiel som leveransen innehåller.

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

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

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

Artikel 49

Överföring av säkerhetsskyddsklassificerade EU-uppgifter till entreprenörer eller bidragsmottagare i tredjestater

Säkerhetsskyddsklassificerade EU-uppgifter ska överföras till entreprenörer och bidragsmottagare i tredjestater i enlighet med säkerhetsbestämmelser som överenskommits mellan kommissionens säkerhetsmyndighet, i egenskap av upphandlande eller bidragsbeviljande myndighet, och den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet i den berörda tredjestat där entreprenören eller bidragsmottagaren är registrerad.

Artikel 50

Hantering av uppgifter som placerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED i samband med säkerhetsskyddsklassificerade kontrakt eller bidragsavtal

1. Skydd av säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED som hanteras eller lagras enligt säkerhetsskyddsklassificerade kontrakt eller bidragsavtal ska vara grundade på principerna om proportionalitet och kostnadseffektivitet.

2. Inget säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande ska krävas inom ramen för säkerhetsskyddsklassificerade kontrakt eller bidragsavtal som inbegriper hantering av uppgifter som inplacerats på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED.

3. När ett kontrakt eller bidragsavtal inbegriper hantering av uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED i ett kommunikations- och informationssystem som drivs av en entreprenör, ska den upphandlande eller bidragsbeviljande myndigheten, efter samråd med kommissionens säkerhetsmyndighet, se till att kontraktet eller bidragsavtalet specificerar de nödvändiga tekniska och administrativa kraven för ackreditering eller godkännande av kommunikations- och informationssystemet i proportion till den uppskattade risken, med beaktande av alla relevanta faktorer. Kommissionens säkerhetsmyndighet och den berörda nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten ska enas om omfattningen av ackrediteringen eller godkännandet av ett sådant system.

KAPITEL 7

UTBYTE AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER MED UNIONENS ÖVRIGA INSTITUTIONER, BYRÅER, ORGAN OCH KONTOR, MED MEDLEMSSTATER OCH MED TREDJESTATER OCH INTERNATIONELLA ORGANISATIONER

Artikel 51

Grundprinciper

1. Om kommissionen eller någon av dess avdelningar fastställer att det finns ett behov av utbyte av säkerhetsskyddsklassificerade EU-uppgifter med unionens övriga institutioner, byråer, organ eller kontor, eller med en tredjestat eller internationell organisation, ska nödvändiga åtgärder vidtas för att inrätta en lämplig rättslig eller administrativ ram för detta ändamål, vilket kan inbegripa informationssäkerhetsavtal eller administrativa överenskommelser som ingåtts i enlighet med relevanta regler.

2. Utan att det påverkar tillämpningen av artikel 57 ska säkerhetsskyddsklassificerade EU-uppgifter endast utbytas med unionens övriga institutioner, byråer, organ eller kontor, eller med en tredjestat eller internationell organisation, under förutsättning att en lämplig rättslig eller administrativ ram finns på plats och att det föreligger tillräckliga garantier för att institutionen, byrån, organet eller kontoret i fråga, eller den berörda tredjestaten eller internationella organisationen, tillämpar likvärdiga grundläggande principer och minimistandarder för skydd av säkerhetsskyddsklassificerade uppgifter.

Artikel 52

Utbyte av säkerhetsskyddsklassificerade EU-uppgifter med unionens övriga institutioner, byråer, organ och kontor

1. Före ingåendet av ett administrativt arrangemang för utbyte av säkerhetsskyddsklassificerade EU-uppgifter med en annan av unionens institutioner, byråer, organ eller kontor ska kommissionen försäkra sig om att institutionen, byrån, organet eller kontoret i fråga

a) har infört ett regelverk för skydd av säkerhetsskyddsklassificerade EU-uppgifter, som fastställer grundläggande principer och miniminormer motsvarande dem som fastställs i detta beslut och dess tillämpningsföreskrifter,

b) tillämpar säkerhetsstandarder och riktlinjer i fråga om personalsäkerhet, fysisk säkerhet, hantering av säkerhetsskyddsklassificerade EU-uppgifter och säkerhet när det gäller kommunikations- och informationssystem, vilka garanterar att säkerhetsskyddsklassificerade EU-uppgifter omfattas av skydd på en nivå motsvarande den som ges inom kommissionen,

c) märker säkerhetsskyddsklassificerade uppgifter som den ger upphov till som säkerhetsskyddsklassificerade EU-uppgifter.

2. Generaldirektoratet för personal och säkerhet ska i nära samarbete med andra behöriga kommissionsavdelningar fungera som huvudansvarig avdelning inom kommissionen för ingående av administrativa arrangemang för utbyte av säkerhetsskyddsklassificerade EU-uppgifter med unionens övriga institutioner, byråer, organ eller kontor.

3. Administrativa arrangemang ska i princip ha formen av en skriftväxling, och undertecknas av generaldirektören för personal och säkerhet på kommissionens vägnar.

4. Före ingåendet av ett administrativt arrangemang om utbyte av säkerhetsskyddsklassificerade EU-uppgifter ska kommissionens säkerhetsmyndighet genomföra ett utvärderingsbesök för att bedöma den rättsliga ramen för skydd av säkerhetsskyddsklassificerade EU-uppgifter och kontrollera ändamålsenligheten av de åtgärder som genomförs för att skydda säkerhetsskyddsklassificerade EU-uppgifter. Den administrativa överenskommelsen ska träda i kraft och säkerhetsskyddsklassificerade EU-uppgifter utbytas endast om resultatet av detta utvärderingsbesök är tillfredsställande och de rekommendationer som lämnats efter besöket har följts. Regelbundna uppföljningsbesök ska genomföras för att kontrollera att det administrativa arrangemanget följs och att de säkerhetsåtgärder som införts fortsätter att uppfylla de grundläggande principer och de minimistandarder som man kommit överens om.

5. Inom kommissionen ska den registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter som förvaltas av generalsekretariatet som regel fungera som huvudsaklig kontaktpunkt för in- och utförsel när det gäller utbyte av säkerhetsskyddsklassificerade uppgifter med andra av unionens institutioner, byråer, organ och kontor. När det av säkerhetsskäl eller av organisatoriska eller operativa skäl är mer lämpligt för att skydda säkerhetsskyddsklassificerade EU-uppgifter, ska lokala registreringsenheter för säkerhetsskyddsklassificerade EU-uppgifter, som inrättats inom kommissionens avdelningar i enlighet med detta beslut och dess tillämpningsföreskrifter, fungera som kontaktpunkt för in- och utförsel för säkerhetsskyddsklassificerade uppgifter rörande frågor som omfattas av de berörda kommissionsavdelningarnas behörighet.

6. Kommissionens grupp av säkerhetsexperter ska underrättas om ingåendet av administrativa arrangemang i enlighet med punkt 2.

Artikel 53

Utbyte av säkerhetsskyddsklassificerade EU-uppgifter med medlemsstater

1. Säkerhetsskyddsklassificerade EU-uppgifter får utbytas med och lämnas ut till medlemsstater under förutsättning att dessa skyddar uppgifterna i enlighet med de krav som gäller för säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsskyddsklassificering på motsvarande nivå i enlighet med jämförelsetabellen för säkerhetsskyddsklassificeringsnivåer i bilaga I.

2. Om medlemsstaterna för in säkerhetsskyddsklassificerade uppgifter med en nationell säkerhetsklassificering i kommissionens strukturer eller nät, ska kommissionen skydda uppgifterna i enlighet med kraven för säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå i enlighet med jämförelsetabellen för säkerhetsskyddsklassificeringsnivåer i bilaga I.

Artikel 54

Utbyte av säkerhetsskyddsklassificerade EU-uppgifter med tredjestater och internationella organisationer

1. När kommissionen fastställer att det finns ett långsiktigt behov av utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater eller internationella organisationer, ska nödvändiga åtgärder vidtas för att inrätta en lämplig rättslig eller administrativ ram för detta ändamål, vilket kan inbegripa informationssäkerhetsavtal eller administrativa överenskommelser som ingåtts i enlighet med relevanta regler.

2. Sådana informationssäkerhetsavtal och administrativa arrangemang som avses i punkt 1 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 minimistandarder som motsvarar de som fastställs i detta beslut.

3. Kommissionen får ingå administrativa arrangemang i enlighet med artikel 56 om säkerhetsskyddsklassificeringsnivån för säkerhetsskyddsklassificerade EU-uppgifter generellt inte är högre än RESTREINT UE/EU RESTRICTED.

4. Sådana administrativa överenskommelser om utbyte av säkerhetsskyddsklassificerade uppgifter som avses i punkt 3 ska innehålla bestämmelser som sörjer för att säkerhetsskyddsklassificerade EU-uppgifter som tredjestater eller internationella organisationer mottar skyddas på ett sätt som är lämpligt med avseende på deras säkerhetsskyddsklassificeringsnivå och i enlighet med minimistandarder som motsvarar de som fastställs i detta beslut. Kommissionens grupp av säkerhetsexperter ska höras om ingåendet av informationssäkerhetsavtal eller administrativa arrangemang.

5. Beslutet att lämna ut säkerhetsskyddsklassificerade EU-uppgifter med upphov i kommissionen till en tredjestat eller internationell organisation ska fattas av berörd kommissionsavdelning, i egenskap av upphovsman inom kommissionen till uppgifterna, från fall till fall med hänsyn till uppgifternas natur och innehåll, mottagarens behovsenliga behörighet och den fördel som unionen vinner därigenom. Om det inte är kommissionen som är upphovsman till de säkerhetsskyddsklassificerade uppgifterna, och kommissionens inte heller är upphovsman till eventuellt källmaterial de kan innehålla, ska den kommissionsavdelning som innehar de säkerhetsskyddsklassificerade uppgifterna först söka upphovsmannens skriftliga medgivande till att lämna ut uppgifterna. Om upphovsmannen inte kan fastställas ska den kommissionsavdelning som innehar dessa säkerhetsskyddsklassificerade uppgifter överta upphovsmannens ansvar efter samråd med kommissionens grupp av säkerhetsexperter.

Artikel 55

Informationssäkerhetsavtal

1. Informationssäkerhetsavtal med tredjeländer eller internationella organisationer ska ingås i enlighet med artikel 218 i EUF-fördraget.

2. Informationssäkerhetsavtal ska

a) fastställa grundprinciper och miniminormer för utbyte av säkerhetsskyddsklassificerade uppgifter mellan unionen och en tredjestat eller internationell organisation,

b) innehålla tekniska genomförandebestämmelser som ska godkännas av behöriga säkerhetsmyndigheter vid relevanta unionsinstitutioner och -organ och den berörda tredjestatens eller internationella organisationens behöriga säkerhetsmyndighet; sådana bestämmelser ska ta hänsyn till den skyddsnivå som erbjuds genom befintliga säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden i den berörda tredjestaten eller internationella organisationen,

c) innehålla bestämmelser om huruvida det, innan säkerhetsskyddsklassificerade uppgifter lämnas ut i enlighet med avtalet, ska bekräftas att den mottagande parten på lämpligt sätt kan skydda säkerhetsskyddsklassificerade uppgifter som lämnas ut till den.

3. När ett behov av att utbyta säkerhetsskyddsklassificerad information har fastställts i enlighet med artikel 51.1 ska kommissionen i lämpliga fall samråda med utrikestjänsten, rådets generalsekretariat och andra unionsinstitutioner och unionsorgan i syfte att avgöra om en rekommendation enligt artikel 218.3 i EUF-fördraget bör avges.

4. Säkerhetsskyddsklassificerade EU-uppgifter får inte utbytas i elektronisk form, såvida detta inte uttryckligen föreskrivs i informationssäkerhetsavtalet eller i de tekniska genomförandebestämmelserna.

5. Inom kommissionen ska den registreringsenhet för säkerhetsskyddsklassificerade EU-uppgifter som förvaltas av generalsekretariatet som regel fungera som huvudsaklig kontaktpunkt för in- och utpassering när det gäller utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer. När det av säkerhetsskäl eller av organisatoriska eller operativa skäl är mer lämpligt för att skydda säkerhetsskyddsklassificerade EU-uppgifter, ska lokala registreringsenheter för säkerhetsskyddsklassificerade EU-uppgifter, som inrättats inom kommissionens avdelningar i enlighet med detta beslut och dess tillämpningsföreskrifter, fungera som kontaktpunkt för in- och utpassering för säkerhetsskyddsklassificerade uppgifter rörande frågor som omfattas av de berörda kommissionsavdelningarnas behörighet.

6. För att bedöma ändamålsenligheten av säkerhetsbestämmelserna, säkerhetsstrukturerna och säkerhetsförfarandena i den berörda tredjestaten eller internationella organisationen ska kommissionen, i samarbete med andra av unionens institutioner, byråer eller organ, delta i utvärderingsbesök, i samförstånd med den berörda tredjestaten eller internationella organisationen. Sådana utvärderingsbesök ska utvärdera

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

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

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

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

Artikel 56

Administrativa överenskommelser

1. När det, inom en unionspolitisk eller unionsrättslig ram, föreligger ett långsiktigt behov av att utbyta säkerhetsskyddsklassificerade uppgifter som i regel inte ligger över säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED med en tredjestat eller internationell organisation, och när kommissionens säkerhetsmyndighet, efter samråd med kommissionens grupp av säkerhetsexperter, har fastställt särskilt att den parten inte har ett tillräckligt utvecklat säkerhetssystem för att ingå ett informationssäkerhetsavtal, får kommissionen besluta om att ingå ett administrativt arrangemang med de berörda myndigheterna i tredjestaten eller den internationella organisationen i fråga.

2. Sådana administrativa arrangemang ska i princip ha formen av en skriftväxling.

3. Ett utvärderingsbesök ska genomföras före ingåendet av avtalet. Kommissionen grupp av säkerhetsexperter ska underrättas om resultatet av utvärderingsbesöket. Om det finns exceptionella skäl för ett brådskande utbyte av säkerhetsskyddsklassificerade uppgifter, får säkerhetsskyddsklassificerade EU-uppgifter lämnas ut under förutsättning att alla ansträngningar görs för att genomföra ett utvärderingsbesök snarast möjligt.

4. Inga säkerhetsskyddsklassificerade EU-uppgifter får utbytas på elektronisk väg, såvida detta inte uttryckligen föreskrivs i den administrativa överenskommelsen.

Artikel 57

Ad hoc-utlämning av säkerhetsskyddsklassificerade EU-uppgifter i undantagsfall

1. Om inget informationssäkerhetsavtal eller administrativt arrangemang finns på plats, och om kommissionen eller någon av dess avdelningar slår fast att det, inom unionens politiska och rättsliga ramar, finns ett exceptionellt behov av att lämna ut säkerhetsskyddsklassificerade EU-uppgifter till en tredjestat eller en internationell organisation, ska kommissionens säkerhetsmyndighet i möjligaste mån kontrollera med säkerhetsmyndigheterna i den berörda tredjestaten eller internationella organisationen att dess säkerhetsbestämmelser, säkerhetsstrukturer och säkerhetsförfaranden garanterar att de säkerhetsskyddsklassificerade EU-uppgifter som kommer att lämnas ut till denna skyddas enligt standarder som är minst lika stränga som dem som fastställs i detta beslut.

2. Beslutet att lämna ut säkerhetsskyddsklassificerade EU-uppgifter till den berörda tredjestaten eller internationella organisationen ska, efter samråd med kommissionens grupp av säkerhetsexperter, fattas av kommissionen på grundval av ett förslag från den kommissionsledamot som ansvarar för säkerhetsfrågor.

3. Efter kommissionens beslut att lämna ut säkerhetsskyddsklassificerade EU-uppgifter ska den behöriga kommissionsavdelningen, med förbehåll för att upphovsmannen, inklusive upphovsmännen till källmaterial som uppgifterna kan innehålla, lämnar sitt skriftliga samtycke, översända uppgifterna i fråga, som ska vara försedda med en markering om att uppgifterna får lämnas ut samt om vilken tredjestat eller internationell organisation de har lämnats ut till. Före eller vid den faktiska utlämningen ska den berörda tredje parten skriftligen åta sig att skydda de mottagna säkerhetsskyddsklassificerade EU-uppgifterna i enlighet med de grundläggande principer och miniminormer som anges i detta beslut.

KAPITEL 8

SLUTBESTÄMMELSER

Artikel 58

Ersättande av föregående beslut

Genom detta beslut upphävs och ersätts kommissionens beslut 2001/844/EG, EKSG, Euratom ([1]).

Artikel 59

Säkerhetsskyddsklassificerade uppgifter som upprättats före ikraftträdandet av detta beslut

1. Alla säkerhetsskyddsklassificerade EU-uppgifter som klassificerats i enlighet med beslut 2001/844/EG, EKSG, Euratom ska även fortsättningsvis skyddas i enlighet med relevanta bestämmelser i det här beslutet.

2. Alla säkerhetsskyddsklassificerade uppgifter som innehades av kommissionen den dag då kommissionens beslut 2001/844/EG, EKSG, Euratom trädde i kraft, med undantag för säkerhetsskyddsklassificerade Euratom-uppgifter, ska

a) om uppgifterna kommer från kommissionen, också fortsättningsvis anses ha omklassificerats automatiskt som RESTREINT UE, såvida inte upphovsmannen hade beslutat om att ge dem en annan klassificering senast den 31 januari 2002 och hade informerat alla adressater för dokumentet i fråga,

b) om uppupphovsmannen inte tillhör kommissionen, behålla den ursprungliga klassificeringen och således behandlas som säkerhetsskyddsklassificerade EU-uppgifter på motsvarande nivå, såvida inte upphovsmannen samtycker till hävande av säkerhetsskyddsklassificeringen eller inplacering på en lägre säkerhetsskyddsklassificeringsnivå.

Artikel 60

Tillämpningsföreskrifter och säkerhetsmeddelanden

1. Om nödvändigt kommer antagandet av tillämpningsföreskrifter för detta beslut att bli föremål för ett separat beslut om delegering från kommissionen till den ledamot av kommissionen som ansvarar för säkerhetsfrågor, i full överensstämmelse med den interna arbetsordningen.

2. Efter att ha bemyndigats genom ovannämnda kommissionsbeslut, får den ledamot av kommissionen som ansvarar för säkerhetsfrågor utarbeta säkerhetsmeddelanden om fastställande av riktlinjer för säkerhet och bästa praxis inom ramen för detta beslut och dess tillämpningsföreskrifter.

3. Kommissionen får delegera de uppgifter som anges i punkterna 1 och 2 i denna artikel till generaldirektören för personal och säkerhet genom ett separat beslut om delegering, i full överensstämmelse med den interna arbetsordningen.

Artikel 61

Ikraftträdande

Detta beslut träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 13 mars 2015.

På kommissionens vägnar

Jean-Claude JUNCKER

Ordförande

([1]) Kommissionens beslut 2001/844/EG, EKSG, Euratom av den 29 november 2001 om ändring av de interna stadgarna (EGT L 317, 3.12.2001, s. 1).

BILAGA I

JÄMFÖRELSETABELL FÖR SÄKERHETSSKYDDSKLASSIFICERINGAR

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgien	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Se fotnot ([1])
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Republiken Tjeckien	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Tyskland	Streng geheim	Geheim	VS ([2]) – Vertraulich	VS – Nur für den Dienstgebrauch
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irland	Top Secret	Secret	Confidential	Restricted
Grekland	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Frankrike	Très Secret Défense	Secret Défense	Confidentiel Défense	Se fotnot ([3])
Kroatien	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Cypern	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungern	”Szigorúan titkos!”	”Titkos!”	”Bizalmas!”	”Korlátozott terjesztésű!”
Malta	L-Għola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nederländerna	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polen	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	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 HEMLIG	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 säkerhetsskyddsklassificering i Belgien. Belgien hanterar och skyddar uppgifter på nivån ”RESTREINT UE/EU RESTRICTED” på ett sätt som inte är mindre strängt är de standarder och förfaranden som beskrivs i Europeiska unionens råds säkerhetsbestämmelser.

([2]) Tyskland: VS = Verschlusssache.

([3]) Frankrike använder inte klassificeringen ”RESTREINT” i sitt nationella system. Frankrike hanterar och skyddar uppgifter på nivån ”RESTREINT UE/EU RESTRICTED” på ett sätt som inte är mindre strängt är de standarder och förfaranden som beskrivs i Europeiska unionens råds säkerhetsbestämmelser.

([4]) Sverige: de övre säkerhetsklassificeringarna används av försvarsmyndigheter och de undre av andra 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.

BILAGA II

FÖRTECKNING OVER FÖRKORTNINGAR

Förkortning	Betydelse
CA	Kryptomyndighet
CAA	Kryptogodkännande myndighet
CCTV	Övervakningskameror
CDA	Kryptodistribueringsmyndighet
CIS	Kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter
DSA	Utsedd säkerhetsmyndighet
EUCI	Säkerhetsskyddsklassificerade EU-uppgifter
FSC	Säkerhetsgodkännande av verksamhetsställe
IA	Informationssäkring
IAA	Myndighet för informationssäkring
IDS	System för upptäckt av intrång
IT	Informationsteknik
LSO	Lokalt säkerhetsansvarig
NSA	Nationell säkerhetsmyndighet
PSC	Personalsäkerhetsgodkännande
PSCC	Intyg om personalsäkerhetsgodkännande
PSI	Säkerhetsanvisningar för program eller projekt
RCO	Kontrolltjänsteman för register
SAA	Myndighet för säkerhetsackreditering
SAL	Säkerhetsskyddsöverenskommelse
SCG	Anvisningar för säkerhetsskyddsklassificering
SecOPs	Säkra driftsmetoder
TA	Tempestmyndighet
TFEU	Fördraget om Europeiska unionens funktionssätt

BILAGA III

FÖRTECKNING OVER NATIONELLA SÄKERHETSMYNDIGHETER

BELGIEN

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
rue des Petits Carmes 15
1000 Bruxelles
Tfn sekretariat: +32 25014542
Fax +32 25014596
E-post: nvo-ans@diplobel.fed.be

BULGARIEN

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tfn +359 29333600
Fax +359 29873750
E-post: dksi@government.bg
Internet: www.dksi.bg

REPUBLIKEN TJECKIEN

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tfn +420 257283335
Fax +420 257283110
E-post: czech.nsa@nbu.cz
Internet: www.nbu.cz

DANMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tfn +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tfn +45 33325566
Fax +45 33931320

TYSKLAND

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin
Tfn +49 30186810
Fax +49 30186811441
E-post: oesIII3@bmi.bund.de

ESTLAND

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tfn +372 7170113 0019, +372 7170117
Fax +372 7170213
E-post: nsa@mod.gov.ee

GREKLAND

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Tfn +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tfn +34 913725000
Fax +34 913725808
E-post: nsa-sp@areatec.com

FRANKRIKE

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tfn +33 171758177
Fax + 33 171758200

KROATIEN

Office of the National Security Council
Croatian NSA
Jurjevska 34
HR-10000 Zagreb
Tfn +385 14681222
Fax + 385 14686049
Internet: www.uvns.hr

IRLAND

National Security Authority
Department of Foreign Affairs
76–78 Harcourt Street
Dublin 2
Tfn +353 14780822
Fax +353 14082959

ITALIEN

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tfn +39 0661174266
Fax +39 064885273

CYPERN

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tfn +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-post: cynsa@mod.gov.cy

LETTLAND

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Tfn +371 67025418
Fax +371 67025454
E-post: ndi@sab.gov.lv

LITAUEN

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tfn +370 70666701, +370 70666702
Fax +370 70666700
E-post: nsa@vsd.lt

LUXEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tfn +352 24782210 central
+352 24782253 direct
Fax +352 24782243

UNGERN

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tfn +36 17952303
Fax +36 17950344

Postadress:
1357 Budapest, PO Box 2
E-post: nbf@nbf.hu
Internet: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tfn +356 21249844
Fax +356 25695321

NEDERLÄNDERNA

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel.: +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tfn +31 703187060
Fax +31 703187522

ÖSTERRIKE

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tfn +43 1531152594
Fax +43 1531152615
E-post: ISK@bka.gv.at

POLEN

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tfn +48 225857944
Fax +48 225857443
E-post: nsa@abw.gov.pl
Internet: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tfn +351 213031710
Fax +351 213031711

RUMÄNIEN

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tfn +40 212245830
Fax +40 212240714
E-post: nsa.romania@nsa.ro
Internet: www.orniss.ro

SLOVENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana
Tfn +386 14781390
Fax +386 14781399
E-post: gp.uvtp@gov.si

SLOVAKIEN

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tfn +421 268692314
Fax +421 263824005
Internet: www.nbusr.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tfn 16055890
Fax +358 916055140
E-post: NSA@formin.fi

SVERIGE

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm
Tfn +46 84051000
Fax +46 87231176
E-post: ud-nsa@foreign.ministry.se

FÖRENADE KUNGARIKET

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tfn 1: +44 2072765649
Tfn 2: +44 2072765497
Fax +44 2072765651
E-post: UK-NSA@cabinet-office.x.gsi.gov.uk