KOMMISSIONENS AFGØRELSE (EU, Euratom) 2019/1963

af 17. oktober 2019

om gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede indkøbskontrakter

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 249,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 106,

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen ([1]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer ([2]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2017/46 af 10. januar 2017 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen ([3]),

efter høring af Kommissionens sikkerhedsekspertgruppe, jf. artikel 41, stk. 5, i afgørelse (EU, Euratom) 2015/444, og

ud fra følgende betragtninger:

(1) I henhold til artikel 41, 42, 47 og 48 i afgørelse (EU, Euratom) 2015/444 skal der fastlægges nærmere bestemmelser til supplering af samme afgørelses kapitel 6 i gennemførelsesbestemmelser om industrisikkerhed, nærmere betegnet udbudsproceduren, indgåelsen af klassificerede kontrakter, facilitetssikkerhedsgodkendelse, personelsikkerhedsgodkendelse, besøg samt transmission og transport af EU-klassificerede informationer (EUCI).

(2) I henhold til afgørelse (EU, Euratom) 2015/444 gennemføres klassificerede kontrakter i tæt samarbejde med den nationale sikkerhedsmyndighed (NSA'en), den udpegede sikkerhedsmyndighed (DSA'en) eller en anden kompetent myndighed i de pågældende medlemsstater. Desuden sikrer hver medlemsstat, at enhver enhed under dens jurisdiktion, som vil kunne frembringe eller modtage klassificerede informationer udstedt af Kommissionen, er behørigt sikkerhedsgodkendt og kan yde en passende beskyttelse på det relevante sikkerhedsniveau ækvivalent med det, der i henhold til Rådet for Den Europæiske Unions regler for sikkerhedsbeskyttelse af EU's klassificerede informationer er forsynet med en tilsvarende klassifikationsmærkning, jf. aftalen mellem Den Europæiske Unions medlemsstater, forsamlet i Rådet, om beskyttelse af klassificerede informationer, som udveksles i Den Europæiske Unions interesse (2011/C 202/05) ([4]).

(3) Rådet, Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik er enige om at sikre størst mulig konsekvens i anvendelsen af sikkerhedsreglerne, hvad angår beskyttelse af EUCI, samtidig med at der tages hensyn til deres specifikke institutionelle og organisatoriske behov i overensstemmelse med de erklæringer, der er knyttet til protokollen for Rådets samling, hvor Rådets afgørelse 2013/488/EU ([5]) om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer blev vedtaget.

(4) Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede kontrakter bør derfor også sikre størst mulig overensstemmelse og tage hensyn til retningslinjerne for industrisikkerhed godkendt af Rådets Sikkerhedsudvalg den 13. december 2016 samt artikel 7 og 22 i Europa-Parlamentets og Rådets direktiv 2009/81/EF ([6]).

(5) Den 4. maj 2016 vedtog Kommissionen en afgørelse ([7]) om bemyndigelse af Kommissionens medlem med ansvar for sikkerhedsanliggender til på Kommissionens vegne og ansvar at vedtage de gennemførelsesbestemmelser, der henvises til i artikel 60 i afgørelse (EU, Euratom) 2015/444 —

([1]) EUT L 72 af 17.3.2015, s. 41.
([2]) EUT L 72 af 17.3.2015, s. 53.
([3]) EUT L 6 af 11.1.2017, s. 40.
([4]) EUT C 202 af 8.7.2011, s. 13.
([5]) Rådets afgørelse 2013/488/EU af 23. september 2013 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 274 af 15.10.2013 s. 1).
([6]) Europa-Parlamentets og Rådets direktiv 2009/81/EF af 13. juli 2009 om samordning af fremgangsmåderne ved ordregivende myndigheders eller ordregiveres indgåelse af visse bygge- og anlægs-, vareindkøbs- og tjenesteydelseskontrakter på forsvars- og sikkerhedsområdet og om ændring af direktiv 2004/17/EF og 2004/18/EF (EUT L 216 af 20.8.2009, s. 76).
([7]) Kommissionens afgørelse af 4.5.2016 om »an empowerment relating to security« (C(2016) 2797 final) (findes ikke på dansk).

VEDTAGET DENNE AFGØRELSE:

KAPITEL 1

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. I denne afgørelse fastsættes gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede indkøbskontrakter til afgørelse (EU, Euratom) 2015/444, særlig kapitel 6 deri.

2. I denne afgørelse fastsættes specifikke krav til erhvervsdrivendes sikkerhedsbeskyttelse af EU-klassificerede informationer (EUCI) forud for indgåelse af kontrakten, i løbet af livscyklussen for klassificerede kontrakter indgået med Europa-Kommissionen og kontrakter med underkontrahenter indgået af Kommissionens kontrahenter.

3. Denne afgørelse vedrører informationer med følgende klassifikationsgrader:

a) RESTREINT UE/EU RESTRICTED

b) CONFIDENTIEL UE/EU CONFIDENTIAL

c) SECRET UE/EU SECRET.

Artikel 2

Kommissionens ansvars

1. Som fastsat i finansforordningen ([8]) er Kommissionens anvisningsberettigede ansvarlig for at sikre, at klassificerede kontrakter henviser til minimumsstandarderne for industrisikkerhed i kapitel 6 i afgørelse (EU, Euratom) 2015/444 samt nærværende gennemførelsesbestemmelser og, hvor det er relevant, i udbudsbekendtgørelsen eller opfordringen til at afgive tilbud og for at sikre, at disse standarder opfyldes under gennemførelsen.

2. Med henblik herpå søger den pågældende anvisningsberettigede i alle faser rådgivning hos Kommissionens sikkerhedsmyndighed om spørgsmål vedrørende sikkerhedsaspekterne ved den klassificerede kontrakt, det klassificerede program eller det klassificerede projekt og underretter den lokale sikkerhedsansvarlige om de kontrakter, der er indgået. Ansvaret for beslutningen om klassifikationsgraden for hvert enkelt emne ligger hos den kontraherende myndighed og træffes under behørigt hensyn til klassifikationsvejledningen (SCG'en).

3. Under hensyntagen til kravene i nærværende gennemførelsesbestemmelser arbejder Kommissionens sikkerhedsmyndighed tæt sammen med de nationale sikkerhedsmyndigheder (NSA'er) og de udpegede sikkerhedsmyndigheder (DSA'er) i de pågældende medlemsstater, navnlig hvad angår facilitetssikkerhedsgodkendelser (FSC'er), personelsikkerhedsgodkendelser (PSC'er), besøgsprocedurer og transportplaner.

KAPITEL 2

HÅNDTERING AF UDBUD VEDRØRENDE KLASSIFICEREDE KONTRAKTER

Artikel 3

Grundprincipper

1. Klassificerede kontrakter tildeles udelukkende erhvervsdrivende, som er registreret i en medlemsstat, eller erhvervsdrivende, som er registreret i et tredjeland eller oprettet af en international organisation, under forudsætning af at det pågældende tredjeland eller den pågældende internationale organisation har indgået en aftale om informationssikkerhed med Den Europæiske Union eller en administrativ ordning med Kommissionen ([9]).

2. Inden der iværksættes et udbud om indgåelse af en klassificeret kontrakt, fastsætter den kontraherende myndighed klassifikationsgraden for de informationer, som måtte blive videregivet til tilbudsgiverne. Den kontraherende myndighed fastsætter også den højeste klassifikationsgrad for informationer, som frembringes i forbindelse med opfyldelsen af kontrakten, programmet eller projektet, eller som minimum den forventede mængde og type informationer, som produceres eller håndteres, og om der er behov for et klassificeret kommunikations- og informationssystem (CIS).

([8]) Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1).

([9]) Listen over aftaler indgået af EU og ordninger indgået af Europa-Kommissionen, i henhold til hvilke EU-klassificerede informationer kan udveksles med tredjelande og internationale organisationer, findes på Kommissionens websted.

3. Den kontraherende myndighed sikrer, at udbudsbekendtgørelser vedrørende klassificerede kontrakter omfatter oplysninger om de særlige sikkerhedsmæssige forpligtelser, der skal opfyldes i forbindelse med klassificerede informationer. Bilag I indeholder et forslag til en skabelon til oplysningerne i udbudsbekendtgørelsen.

4. Den kontraherende myndighed sikrer, at informationer klassificeret RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET først gøres tilgængelige for tilbudsgiverne, når de har underskrevet en fortrolighedsaftale, som forpligter tilbudsgiverne til at håndtere og beskytte EUCI i henhold til afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil.

5. Alle kontrahenter, som skal håndtere eller lagre informationer klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET på deres faciliteter, enten i forbindelse med opfyldelsen af den klassificerede kontrakt eller i perioden forud for indgåelse af kontrakten, skal være i besiddelse af en FSC på det krævede niveau. Følgende beskriver de tre scenarier, der kan opstå i forbindelse med tilbudsfasen for en klassificeret kontrakt, som omfatter EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET:

a) Ingen adgang til EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i tilbudsfasen:

   Hvis udbudsbekendtgørelsen eller opfordringen til at afgive tilbud vedrører en kontrakt, som vil indebære adgang til EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, men som ikke kræver, at tilbudsgiveren håndterer sådanne informationer i tilbudsfasen, må en tilbudsgiver, der ikke er i besiddelse af en FSC på det krævede niveau, ikke udelukkes fra tilbudsproceduren under henvisning til, at denne ikke er i besiddelse af en FSC.

b) Adgang til EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i tilbudsfasen på den kontraherende myndigheds lokaliteter:

   Der gives adgang til de af tilbudsgivers ansatte, der er i besiddelse af en PSC på det krævede niveau, hvis de har et need to know. Før en sådan adgang gives, verificerer den kontraherende myndighed, gennem Kommissionens sikkerhedsmyndighed, hos de respektive NSA'er/DSA'er om der i henhold til nationale love og forskrifter også kræves en FSC i denne fase.

c) Håndtering eller lagring af EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i tilbudsfasen på tilbudsgiverens lokaliteter:

   Hvis udbudsbekendtgørelsen eller opfordringen til at afgive tilbud kræver, at tilbudsgiveren håndterer eller lagrer EUCI på sine lokaliteter, skal tilbudsgiveren være i besiddelse af en FSC på det krævede niveau. I sådanne tilfælde indhenter den kontraherende myndighed, gennem Kommissionens sikkerhedsmyndighed, en erklæring hos den relevante NSA/DSA som sikkerhed for, at tilbudsgiveren er blevet tildelt en FSC på passende niveau. Der gives adgang til de af tilbudsgivers ansatte, der er i besiddelse af en PSC på det krævede niveau, hvis de har et need to know.

6. I princippet bør der ikke kræves en FSC for at få adgang til RESTREINT UE/EU RESTRICTED-informationer, hverken i tilbudsfasen eller i forbindelse med opfyldelsen af kontrakten. Hvis en medlemsstat kræver en FSC i forbindelse med kontrakter eller underkontrakter med klassifikationsgraden RESTREINT UE/EU RESTRICTED i henhold til medlemsstatens nationale love og forskrifter, jf. bilag IV, må disse nationale krav ikke medføre yderligere forpligtelser for andre medlemsstater eller ekskludere tilbudsgivere, kontrahenter eller underkontrahenter fra medlemsstater, som ikke stiller sådanne FSC-krav for adgang til RESTREINT UE/EU RESTRICTED-informationer, i forbindelse med relaterede kontrakter/underkontrakter eller en udbudsprocedure vedrørende sådanne. Sådanne kontrakter opfyldes i medlemsstaterne i henhold til de nationale love og forskrifter.

7. Hvis der kræves en FSC til opfyldelse af en klassificeret kontrakt, fremsender den kontraherende myndighed, gennem Kommissionens sikkerhedsmyndighed, en anmodning til kontrahentens NSA/DSA i form af et FSC-oplysningsskema. Bilag III, tillæg D, indeholder et eksempel på et FSC-oplysningsskema ([10]). En klassificeret kontrakt tildeles først, når kontrahentens NSA/DSA har bekræftet, at tilbudsgiveren er i besiddelse af en FSC. Der gives så vidt muligt svar på fremsendelsen af et FSC-oplysningsskema inden for ti arbejdsdage fra anmodningsdatoen.

([10]) Andre anvendte skemaer adskiller sig muligvis fra eksemplet i disse gennemførelsesbestemmelser for så vidt angår udformning.

Artikel 4

Underentreprise i forbindelse med klassificerede kontrakter

1. De betingelser, hvorpå en kontrahent, der tildeles en klassificeret kontrakt med Kommissionen, kan udbyde dele af kontrakten i underentreprise, fastsættes i opfordringen til at afgive tilbud og i udbudsdokumenterne. Hvis det i henhold til en klassificeret kontrakt er tilladt at udbyde dele af den i underentreprise, skal den kontraherende myndighed forud herfor give skriftligt samtykke hertil. Inden et sådant samtykke gives, hører den kontraherende myndighed Kommissionens sikkerhedsmyndighed.

2. Klassificerede kontrakter udbydes udelukkende i underentreprise til erhvervsdrivende, som er registreret i en medlemsstat, eller erhvervsdrivende, som er registreret i et tredjeland eller oprettet af en international organisation, under forudsætning af at det pågældende tredjeland eller den pågældende internationale organisation har indgået en aftale om informationssikkerhed med Den Europæiske Union eller en administrativ ordning med Kommissionen ([11]).

KAPITEL 3

TILDELING AF EN KLASSIFICERET KONTRAKT MED KOMMISSIONEN

Artikel 5

Grundprincipper

1. Ved tildelingen af en klassificeret kontrakt sikrer den kontraherende myndighed sammen med Kommissionens sikkerhedsmyndighed, at kontrahentens forpligtelser for så vidt angår sikkerhedsbeskyttelse af EUCI, der videregives til den pågældende kontrahent eller frembringes i forbindelse med opfyldelsen af kontrakten er indarbejdet i kontrakten. Kontraktspecifikke sikkerhedskrav fremgår af de særlige sikkerhedsbetingelser (SAL). Bilag III indeholder et forslag til en SAL-skabelon.

2. Inden den kontraherende myndighed underskriver en klassificeret kontrakt, udarbejder den, efter at have hørt Kommissionens sikkerhedsmyndighed, en klassifikationsvejledning (SCG) med henblik på de opgaver, der skal udføres, og de informationer, der frembringes i forbindelse med opfyldelsen af kontrakten, programmet eller projektet. SCG'en skal indgå i SAL.

3. Program- eller projektspecifikke sikkerhedskrav fastlægges i en program- eller projektsikkerhedsinstruktion (PSI). PSI'en kan udarbejdes ved hjælp af bestemmelserne i SAL-skabelonen i bilag III. PSI'en udarbejdes af den Kommissionstjenestegren, der forvalter programmet eller projektet, i tæt samarbejde med Kommissionens sikkerhedsmyndighed og forelægges Kommissionens sikkerhedsekspertgruppe med henblik på rådgivning. Hvis en kontrakt er en del af et program eller et projekt, der har sin egen PSI, udarbejdes kontraktens SAL i forenklet form med en henvisning til sikkerhedsbestemmelserne i programmets eller projektets PSI.

4. Den kontraherende myndighed anses for at være udstederen af de klassificerede informationer, som udarbejdes eller håndteres i forbindelse med opfyldelsen af kontrakten.

5. Den kontraherende myndighed underretter via Kommissionens sikkerhedsmyndighed alle kontrahenters og underkontrahenters NSA'er/DSA'er om indgåelsen af klassificerede kontrakter eller underkontrakter samt forlængelser eller førtidig afslutning af sådanne kontrakter eller underkontrakter. Bilag IV indeholder en liste over nationale krav.

6. Kontrakter, som omfatter informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal indeholde en kontraktsikkerhedsklausul, der gør bestemmelserne i bilag III, tillæg E, bindende for kontrahenten. Sådanne kontrakter skal indeholde SAL, der som minimum fastsætter kravene til håndtering af RESTREINT UE/EU RESTRICTED-informationer, herunder krav vedrørende informationssikring og specifikke krav, som skal opfyldes af kontrahenter, der handler efter fuldmagt fra den kontraherende myndighed, med henblik på akkreditering af kontrahentens CIS, der håndterer RESTREINT UE/EU RESTRICTED-informationer.

([11]) Listen over aftaler indgået af EU og ordninger indgået af Europa-Kommissionen, i henhold til hvilke EU-klassificerede informationer kan udveksles med tredjelande og internationale organisationer, findes på Kommissionens websted.

7. Hvis RESTREINT UE/EU RESTRICTED-informationer skal videregives til tilbudsgivere eller mulige kontrahenter, indarbejdes minimumskravene i stk. 6 i tilbuddene eller i de relevante fortrolighedsaftaler, der indgås i tilbudsfasen.

8. Hvis det kræves i henhold til de nationale love og forskrifter i en medlemsstat, sikrer NSA'en/DSA'en, at kontrahenter og underkontrahenter under dennes jurisdiktion overholder de gældende sikkerhedsbestemmelser vedrørende sikkerhedsbeskyttelsen af RESTREINT UE/EU RESTRICTED-informationer, og gennemfører kontrolbesøg på kontrahentens faciliteter på medlemsstatens område. Hvis NSA'en/DSA'en ikke er forpligtet hertil, sikrer den kontraherende myndighed, at kontrahenten implementerer de krævede sikkerhedsbestemmelser som fastsat i bilag III.

Artikel 6

Kontrahentens og underkontrahentens ansattes adgang til EUCI

1. I sin kapacitet af kontraherende myndighed sikrer Kommissionstjenestegrenen, at klassificerede kontrakter indeholder bestemmelser om, at en kontrahents eller underkontrahents ansatte, der med henblik på opfyldelsen af den klassificerede kontrakt eller underentreprisekontrakt har behov for adgang til EUCI, kun indrømmes adgang, hvis:

a) det er fastslået, at der er et need to know

b) de for så vidt angår informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, har en PSC på det relevante niveau udstedt af deres respektive NSA/DSA eller en anden kompetent sikkerhedsmyndighed

c) de er blevet orienteret om reglerne og procedurerne for sikkerhedsbeskyttelse af EUCI og har anerkendt deres ansvar med hensyn til beskyttelse af sådanne informationer.

2. Hvis en kontrahent eller underkontrahent ønsker at ansætte en ikke-EU-borger i en stilling, som kræver adgang til EUCI, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, er det kontrahentens eller underkontrahentens ansvar at igangsætte proceduren for sikkerhedsgodkendelse af den pågældende person i overensstemmelse med de nationale love og forskrifter, der gælder for den facilitet, hvor der skal gives adgang til EUCI.

KAPITEL 4

BESØG I FORBINDELSE MED KLASSIFICEREDE KONTRAKTER

Artikel 7

Grundprincipper

1. Hvis Kommissionen, kontrahenter eller underkontrahenter skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, på hinandens lokaliteter med henblik på opfyldelse af en klassificeret kontrakt, arrangeres sådanne besøg i samråd med de pågældende NSA'er/DSA'er eller en anden kompetent sikkerhedsmyndighed.

2. Der gælder følgende krav i forbindelse med de i stk. 1 omhandlede besøg:

a) besøget skal have et officielt formål, der vedrører en klassificeret kontrakt tildelt af Kommissionen

b) alle besøgende skal have en PSC på det krævede niveau og et need to know for at få adgang til EUCI, der videregives eller frembringes i forbindelse med opfyldelsen af den af Kommissionen tildelte kontrakt.

Artikel 8

Besøgsanmodninger

1. Kontrahenters besøg på andre kontrahenters faciliteter eller Kommissionens lokaliteter, som indebærer adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, arrangeres efter følgende procedure:

a) den sikkerhedsansvarlige for den facilitet, der sender den besøgende, udfylder alle relevante dele af besøgsanmodningen og indgiver den til sin facilitets NSA/DSA. Bilag III, tillæg C, indeholder en skabelon til besøgsanmodninger

b) NSA'en/DSA'en for den facilitet, der sender den besøgende, bekræfter den besøgendes PSC, før besøgsanmodningen fremsendes til NSA'en/DSA'en for den facilitet, som skal besøges, (eller til Kommissionens sikkerhedsmyndighed, hvis der er tale om et besøg på Kommissionens lokaliteter)

c) den sikkerhedsansvarlige for den facilitet, der sender den besøgende, modtager derpå via sin egen NSA/DSA svaret fra NSA'en/DSA'en for den facilitet, som skal besøges, (eller Kommissionens sikkerhedsmyndighed), der enten godkender eller afslår besøgsanmodningen

d) en besøgsanmodning anses for godkendt, såfremt der ikke foreligger indsigelser senest fem arbejdsdage før dagen for besøget.

2. Kommissionens tjenestemænds besøg på kontrahenters faciliteter, som indebærer adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, arrangeres efter følgende procedure:

a) den besøgende udfylder alle relevante dele af besøgsanmodningen og indgiver den til Kommissionens sikkerhedsmyndighed

b) Kommissionens sikkerhedsmyndighed bekræfter den besøgendes PSC, før besøgsanmodningen fremsendes til NSA'en/DSA'en for den facilitet, som skal besøges

c) Kommissionens sikkerhedsmyndighed modtager derpå svaret fra NSA'en/DSA'en for den facilitet, som skal besøges, der enten godkender eller afslår besøgsanmodningen

d) en besøgsanmodning anses for godkendt, såfremt der ikke foreligger indsigelser senest fem arbejdsdage før dagen for besøget.

3. En besøgsanmodning kan dække et enkelt eller gentagne besøg. Hvis der er tale om gentagne besøg, kan besøgsanmodningen gælde i op til et år fra den anmodede startdato.

4. En besøgsanmodnings gyldighedsperiode kan ikke gå ud over gyldighedsperioden for den besøgendes PSC.

5. Som hovedregel indgives en besøgsanmodning til de kompetente sikkerhedsmyndigheder for den facilitet, som skal besøges, senest 15 arbejdsdage før dagen for besøget.

Artikel 9

Besøgsprocedurer

1. For at en besøgende gives adgang til EUCI skal sikkerhedskontoret på den facilitet, som besøges, overholde alle besøgsrelaterede sikkerhedsprocedurer og -regler som fastsat af facilitetens NSA/DSA.

2. Besøgende dokumenterer deres identitet ved ankomsten til den facilitet, som besøges, ved fremvisning af gyldigt ID-kort eller pas. Identifikationsoplysningerne skal svare til de oplysninger, der er angivet i besøgsanmodningen.

3. Den facilitet, som besøges, sikrer, at alle besøgende registreres, herunder med navn, den organisation, de repræsenterer, udløbsdatoen for PSC'en, datoen for besøget og navnene på de personer, der besøges. Sådanne optegnelser opbevares i en periode på mindst fem år, eller længere såfremt det kræves i henhold til nationale regler og forskrifter i det land, hvor den facilitet, der besøges, er beliggende.

Artikel 10

Besøg, der arrangeres direkte

1. I forbindelse med specifikke projekter kan de relevante NSA'er/DSA'er og Kommissionens sikkerhedsmyndighed aftale en procedure, hvorved besøg vedrørende en specifik klassificeret kontrakt kan arrangeres direkte mellem den besøgendes sikkerhedsansvarlige og den sikkerhedsansvarlige for den facilitet, som skal besøges. Bilag III, tillæg C, indeholder en skabelon til besøgsanmodningen, som anvendes med henblik herpå. En sådan særlig procedure fastlægges i PSI'en eller andre særlige ordninger. I sådanne tilfælde finder procedurerne i artikel 8 og artikel 9, stk. 1, ikke anvendelse.

2. Besøg, som indebærer adgang til informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, arrangeres direkte mellem den facilitet, der sender den besøgende, og den facilitet, der skal besøges, idet det ikke er nødvendigt at følge procedurerne i artikel 8 og artikel 9, stk. 1.

KAPITEL 5

TRANSMISSION OG TRANSPORT AF EUCI I FORBINDELSE MED OPFYLDELSEN AF KLASSIFICEREDE KONTRAKTER

Artikel 11

Grundprincipper

Den kontraherende myndighed sikrer, at alle beslutninger om transmission og transport af EUCI er i overensstemmelse med afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil og med vilkårene for den klassificerede kontrakt, herunder udstederens samtykke.

Artikel 12

Elektronisk håndtering

1. Elektronisk håndtering og transmission af EUCI foretages i overensstemmelse med bestemmelserne i kapitel 5 og 6 i afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil.

Kommunikations- og informationssystemer, som ejes af en kontrahent og bruges til at håndtere EUCI i forbindelse med opfyldelsen af en kontrakt (kontrahentens CIS) akkrediteres af den ansvarlige sikkerhedsakkrediteringsmyndighed (SAA). Elektroniske transmissioner af EUCI beskyttes af kryptoprodukter, der er godkendt i overensstemmelse med artikel 36, stk. 4, i afgørelse (EU, Euratom) 2015/444. Der gennemføres TEMPEST-foranstaltninger i henhold til artikel 36, stk. 6, i nævnte afgørelse.

2. Sikkerhedsakkrediteringen af en kontrahents CIS, som bruges til at håndtere EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED og eventuelle sammenkoblinger kan uddelegeres til en kontrahents sikkerhedsansvarlige, såfremt dette er tilladt i henhold til nationale love og forskrifter. Hvis denne opgave er uddelegeret, er kontrahenten ansvarlig for at gennemføre de minimumssikkerhedskrav, der er beskrevet i SAL, når RESTREINT UE/EU RESTRICTED-informationer håndteres af dennes CIS. De relevante NSA'er/DSA'er og SAA'er har imidlertid stadig ansvaret for at sikkerhedsbeskytte RESTREINT UE/EU RESTRICTED-informationer, som håndteres af kontrahenten, samt retten til at kontrollere de sikkerhedsforanstaltninger, som kontrahenten har truffet. Desuden afleverer kontrahenten en erklæring til den kontraherende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente nationale SAA, som certificerer, at kontrahentens CIS og relaterede sammenkoblinger er akkrediteret til håndtering af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED ([12]).

Artikel 13

Transport med kurertjenester

Transport af EUCI med kurertjenester skal overholde de relevante bestemmelser i Kommissionens afgørelser om gennemførelsesbestemmelser om håndtering af RESTREINT UE/EU RESTRICTED- og CONFIDENTIEL UE/EU CONFIDENTIAL-informationer.

Artikel 14

Håndbåren transport

1. Håndbåren transport af klassificerede informationer er underlagt strenge sikkerhedskrav.

2. Håndbåren transport af RESTREINT UE/EU RESTRICTED-informationer, må udføres af kontrahentens ansatte inden for EU, forudsat at følgende krav er opfyldt:

a) kuverten eller emballagen er ugennemsigtig og indeholder ingen angivelse af indholdets klassifikationsgrad

([12]) Minimumskravene til kommunikations- og informationssystemer (CIS) til håndtering af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED er fastsat i bilag III, tillæg E.

b) de klassificerede informationer må ikke forlade bæreren

c) kuverten eller emballagen må ikke åbnes undervejs.

3. Håndbåren transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, kan udføres af kontrahentens ansatte inden for en EU-medlemsstat og arrangeres på forhånd mellem den facilitet, der sender informationerne, og den facilitet, der skal modtage informationerne. Den myndighed eller facilitet, der sender informationerne, meddeler den myndighed eller facilitet, der modtager informationerne, de nærmere oplysninger om forsendelsen, herunder referencenummer, klassifikation, forventet ankomsttidspunkt og kurerens navn. Sådan håndbåren transport er tilladt, forudsat at følgende krav er opfyldt:

a) de klassificerede informationer transporteres i en dobbelt kuvert eller emballage

b) den yderste kuvert eller emballage er sikret og indeholder ingen angivelse af indholdets klassifikationsgrad, mens den inderste kuvert er påført klassifikationsgraden

c) EUCI må ikke forlade bæreren

d) kuverten eller emballagen må ikke åbnes undervejs

e) kuverten eller emballagen transporteres i en dokumentmappe, der kan låses, eller i en tilsvarende godkendt beholder, der har en størrelse og en vægt, der gør, at bæreren kan have den på sig hele tiden, og at den ikke skal indskrives som bagage

f) kureren er i besiddelse af et kurercertifikat udstedt af dennes kompetente sikkerhedsmyndighed, som bekræfter, at kureren er autoriseret til at transportere den klassificerede forsendelse som identificeret ovenfor.

4. Hvad angår håndbåren transport af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, fra én medlemsstat til en anden medlemsstat, som udføres af kontrahentens ansatte, gælder desuden følgende yderligere regler:

a) kureren er ansvarlig for, at det klassificerede materiale, der transporteres, opbevares sikkert, indtil det videregives til modtageren

b) hvis der opstår en sikkerhedsbrist, kan afsenderens NSA/DSA anmode om, at myndighederne i det land, hvor sikkerhedsbristen fandt sted, efterforsker sagen, informerer om resultatet af efterforskningen og indleder en retssag eller træffer andre passende foranstaltninger

c) kureren orienteres om alle de sikkerhedsmæssige forpligtelser, der skal overholdes i forbindelse med transporten, og underskriver en erklæring herom

d) instrukserne til kureren vedhæftes kurercertifikatet

e) kureren udstyres med en beskrivelse af forsendelsen og en rejseplan

f) dokumenterne returneres til den udstedende NSA/DSA ved rejsens/rejsernes afslutning eller holdes tilgængelige af modtageren med henblik på overvågning

g) hvis toldmyndigheder, immigrationsmyndigheder eller grænsepoliti beder om at få lov til at undersøge og inspicere forsendelsen, gives de tilladelse til at åbne og se så tilstrækkeligt meget af forsendelsen til, at de kan fastslå, at den ikke indeholder andet materiale end det angivne

h) toldmyndighederne bør anmodes om at respektere den offentlige myndighed, der har udstedt forsendelsesdokumenterne og kurerens autorisationsdokumenter.

Hvis en forsendelse åbnes af toldmyndighederne, bør dette ske således, at uautoriserede personer ikke kan se indholdet, og om muligt i kurerens nærvær. Kureren anmoder om, at forsendelsen pakkes om, og beder de myndigheder, der udfører inspektionen, om at forsegle forsendelsen på ny samt skriftligt bekræfte, at de har åbnet den.

5. Håndbåren transport af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET, til et tredjeland eller en international organisation, som udføres af kontrahentens ansatte, er omfattet af bestemmelserne i aftalen om informationssikkerhed eller den administrative ordning, der er indgået mellem henholdsvis Den Europæiske Union eller Kommissionen og det pågældende tredjeland eller den pågældende internationale organisation.

KAPITEL 6

KONTINUITETSPLANLÆGNING

Artikel 15

Beredskabsplaner og genoprettende foranstaltninger

Kommissionstjenestegrenen sikrer i sin kapacitet af kontraherende myndighed, at klassificerede kontrakter indeholder bestemmelser om, at en kontrahent udarbejder beredskabsplaner til sikkerhedsbeskyttelse af EUCI, der håndteres i forbindelse med opfyldelsen af den klassificerede kontrakt, i tilfælde af en nødsituation og træffer forebyggende og genoprettende foranstaltninger som led i kontinuitetsplanlægningen med henblik på at minimere virkningen af hændelser relateret til håndtering og lagring af EUCI. Kontrahenten meddeler den kontraherende myndighed sin beredskabsplan.

Artikel 16

Ikrafttræden

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 17. oktober 2019.

På Kommissionens vegne

For formanden

Günther OETTINGER

Medlem af Kommissionen

BILAG I

Standardoplysninger i udbudsbekendtgørelser

(tilpasses den pågældende udbudsbekendtgørelse)

Kontrakter, som omfatter informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET

Andre særlige betingelser (*hvis relevant*)

Der gælder særlige betingelser for opfyldelsen af kontrakten ● ja ○ nej

(*hvis ja*) Beskrivelse af de særlige betingelser:

Kontrakten indebærer adgang til, håndtering og/eller lagring af informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, og som er omfattet af reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer fastsat i afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil [1].

Der kræves en facilitetssikkerhedsgodkendelse samt personelsikkerhedsgodkendelser for de af kontrahentens ansatte, der håndterer klassificerede informationer.

Kontrakten vil omfatte særlige sikkerhedsmæssige forpligtelser (jf. de særlige sikkerhedsbetingelser (SAL), der er vedhæftet kontrakten). Den kontraherende myndighed skal give skriftligt samtykke til, at dele af kontrakten udbydes i underentreprise, og underkontrahenten og dennes ansatte skal overholde alle reglerne om sikkerhedsbeskyttelse.

Kontrakter, som omfatter informationer, der er klassificeret RESTREINT UE/EU RESTRICTED

Andre særlige betingelser (*hvis relevant*)

Der gælder særlige betingelser for opfyldelsen af kontrakten ● ja ○ nej

(*hvis ja*) Beskrivelse af de særlige betingelser:

Kontrakten indebærer eller medfører adgang til, håndtering og/eller lagring af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, og som er omfattet af reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer fastsat i afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil [2].

Kontrakten vil omfatte særlige sikkerhedsmæssige forpligtelser (jf. de særlige sikkerhedsbetingelser (SAL), der er vedhæftet kontrakten). Den kontraherende myndighed skal give skriftligt samtykke til, at dele af kontrakten udbydes i underentreprise, og underkontrahenten og dennes ansatte skal overholde alle reglerne om sikkerhedsbeskyttelse.

---

[1] Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.
[2] Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.

BILAG II

STANDARDKLAUSULER I INDKØBSKONTRAKTER

(tilpasses den pågældende kontrakt)

ARTIKEL XX

SIKKERHEDSMÆSSIGE FORPLIGTELSER

XX.1 EU-klassificerede oplysninger

Hvis opfyldelsen af kontrakten indebærer anvendelse eller frembringelse af EU-klassificerede informationer, skal sådanne informationer behandles i overensstemmelse med de særlige sikkerhedsbetingelser (SAL) og klassifikationsvejledningen (SCG) som fastsat i bilag 1 samt Kommissionens afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil ([1]), indtil de er blevet afklassificeret.

Ethvert produkt, der indeholder klassificerede informationer, skal leveres i overensstemmelse med de særlige procedurer, der er aftalt med den kontraherende myndighed.

Projektopgaver, der indebærer klassificerede informationer, må ikke udbydes i underentreprise uden forudgående udtrykkelig skriftlig godkendelse fra den kontraherende myndighed.

EU-klassificerede informationer må ikke videregives til en tredjepart (heriblandt underkontrahenter) uden forudgående skriftlig godkendelse fra den kontraherende myndighed.

([1]) Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.

BILAG III

[Bilag IV (til rammekontrakten)]

SÆRLIGE SIKKERHEDSBETINGELSER (SAL)

[standardskabelon]

Tillæg A

SIKKERHEDSKRAV

Den kontraherende myndighed skal indarbejde følgende sikkerhedskrav i de særlige sikkerhedsbetingelser (SAL). Nogle af klausulerne gælder muligvis ikke for den pågældende kontrakt. I så fald er de omgivet af kantede parenteser.

Listen over klausuler er ikke udtømmende. Der kan tilføjes yderligere klausuler afhængig af typen af klassificeret kontrakt.

ALMINDELIGE BETINGELSER

[N.B.: *gælder for alle klassificerede kontrakter*]

1. Nærværende særlige sikkerhedsbetingelser (SAL) er en integreret del af den klassificerede kontrakt [eller underkontrakt] og angiver de kontraktspecifikke sikkerhedskrav. Manglende opfyldelse af disse krav kan udgøre tilstrækkelig grund til opsigelse af kontrakten.

2. Alle kontrahenter er omfattet af forpligtelserne i afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelser dertil ([1]).

3. Klassificerede informationer, der frembringes under opfyldelse af kontrakten, skal mærkes som EU-klassificerede informationer (EUCI) på sikkerhedsklassifikationsniveau som fastsat i klassifikationsvejledningen (SCG) i tillæg B til nærværende betingelser. Det er kun tilladt at afvige fra klassifikationsgraderne i SCG efter skriftlig autorisation fra den kontraherende myndighed.

4. Rettigheder tilhørende en udsteder af EUCI, der udarbejdes og håndteres i forbindelse med opfyldelsen af en klassificeret kontrakt, udøves af Kommissionen som kontraherende myndighed.

5. Hvis den kontraherende myndighed ikke har givet skriftlig godkendelse hertil, må kontrahenten eller underkontrahenten ikke gøre brug af informationer eller materiale fremskaffet af den kontraherende myndighed eller produceret på vegne af denne myndighed til andre formål, end de i kontrakten anførte.

6. Kontrahenten skal undersøge alle sikkerhedsbrister, der vedrører EUCI, og indberette dem til den kontraherende myndighed så hurtigt som praktisk muligt. Kontrahenten eller underkontrahenten skal straks indberette alle sager, hvor det er kendt, eller der er grund til at formode, at EUCI, der er videregivet eller frembragt i forbindelse med kontrakten, er bortkommet eller videregivet til uautoriserede personer, til sin ansvarlige nationale sikkerhedsmyndighed (NSA) eller til den udpegede sikkerhedsmyndighed (DSA) og, hvis de nationale love og forskrifter tillader det, til Kommissionens sikkerhedsmyndighed.

7. Når kontrakten udløber, skal kontrahenten eller underkontrahenten returnere alle EUCI, som vedkommende er i besiddelse af, til den kontraherende myndighed så hurtigt som muligt. Hvis det er mere praktisk, kan kontrahenten eller underkontrahenten destruere de pågældende EUCI i stedet for at returnere dem. Dette skal ske i overensstemmelse med de nationale love og forskrifter i det land, hvor kontrahenten er baseret, efter forudgående aftale med Kommissionens sikkerhedsmyndighed og i henhold til dennes instrukser. EUCI skal destrueres på en sådan måde, at de ikke kan rekonstrueres, hverken helt eller delvist.

8. Hvis kontrahenten eller underkontrahenten har autorisation til at beholde EUCI efter kontraktens ophævelse eller opfyldelse, skal de pågældende EUCI fortsat beskyttes i henhold til afgørelse (EU, Euratom) 2015/444 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (herefter benævnt »afgørelse 2015/444«) og gennemførelsesbestemmelserne dertil ([2]).

9. Elektronisk håndtering, behandling og transmission af EUCI skal ske i overenssemmelse med bestemmelserne i kapitel 5 og 6 i afgørelse 2015/444. Disse kapitler omfatter bl.a. krav om, at kommunikations- og informationssystemer, som ejes af kontrahenten og bruges til at håndtere EUCI i forbindelse med opfyldelsen af kontrakten (herefter benævnt »kontrahentens CIS«), skal akkrediteres ([3]), at elektronisk transmission af EUCI skal beskyttes af kryptoprodukter, der er godkendt i overensstemmelse med artikel 36, stk. 4, i afgørelse 2015/444, og at der skal gennemføres TEMPEST-foranstaltninger i henhold til artikel 36, stk. 6, i Kommissionens afgørelse 2015/444.

([1]) Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.
([2]) Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.
([3]) Den part, der foretager akkrediteringen, skal aflevere en overensstemmelseserklæring til den kontraherende myndighed via Kommissionens sikkerhedsmyndighed og i samarbejde med den relevante nationale sikkerhedsakkrediteringsmyndighed (SAA).

10. Kontrahenten eller underkontrahenten skal have beredskabsplaner til sikkerhedsbeskyttelse af EUCI, der håndteres i forbindelse med opfyldelsen af den klassificerede kontrakt, i tilfælde af en nødsituation og træffe forebyggende og genoprettende foranstaltninger med henblik på at minimere virkningen af hændelser relateret til håndtering og lagring af EUCI. Kontrahenten eller underkontrahenten skal meddele den kontraherende myndighed sin beredskabsplan.

KONTRAKTER, SOM KRÆVER ADGANG TIL INFORMATIONER, DER ER KLASSIFICERET RESTREINT UE/EU RESTRICTED

11. Der kræves ingen personelsikkerhedsgodkendelse (PSC) i forbindelse med overholdelsen af denne kontrakt. Informationer eller materiale, der er klassificeret RESTREINT UE/EU RESTRICTED, må imidlertid kun være tilgængeligt for de af kontrahentens ansatte, som har behov herfor med henblik på opfyldelsen af kontrakten (need to know-princippet), som af kontrahentens sikkerhedsansvarlige er blevet orienteret om deres ansvar og om konsekvenserne af sikkerhedskompromittering eller sikkerhedsbrud i relation til sådanne informationer, og som skriftligt har anerkendt konsekvenserne af manglende beskyttelse af EUCI.

12. Medmindre den kontraherende myndighed har givet skriftlig godkendelse hertil, må kontrahenten eller underkontrahenten ikke give andre enheder eller personer end de af dennes ansatte, der har et need to know, adgang til informationer eller materiale, der er klassificeret RESTREINT UE/EU RESTRICTED.

13. Kontrahenten eller underkontrahenten skal bevare klassifikationsmærkningerne på klassificerede informationer, der frembringes af eller viderebringes under opfyldelsen af en kontrakt, og må ikke afklassificere informationer uden skriftligt samtykke fra den kontraherende myndighed.

14. Informationer eller materiale, der er klassificeret RESTREINT UE/EU RESTRICTED, skal opbevares i låste kontormøbler, når de ikke anvendes. Når de befinder sig i transit, skal de transporteres i en ugennemsigtig kuvert. Dokumenterne må ikke forlade bæreren og kuverten eller emballagen må ikke åbnes undervejs.

15. Kontrahenten eller underkontrahenten må sende dokumenter, der er klassificeret RESTREINT UE/EU RESTRICTED, til Kommissionen med kommercielle kurervirksomheder og posttjenester, foretage håndbåret transport eller udveksle dem elektronisk. Med henblik herpå skal kontrahenten eller underkontrahenten følge programmets eller projektets sikkerhedsinstruktion (PSI) som udstedt af Kommissionen og/eller Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede indkøbskontrakter ([4]).

16. Når de ikke længere skal bruges, skal dokumenter, der er klassificeret RESTREINT UE/EU RESTRICTED, destrueres på en sådan måde, at de ikke kan rekonstrueres, hverken helt eller delvist.

17. Sikkerhedsakkrediteringen af en kontrahents CIS, som bruges til at håndtere EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED, og eventuelle sammenkoblinger kan uddelegeres til en kontrahents sikkerhedsansvarlige, såfremt dette er tilladt i henhold til nationale love og forskrifter. Selv om akkrediteringen er uddelegeret, har de relevante NSA'er/DSA'er og SAA'er imidlertid stadig ansvaret for at sikkerhedsbeskytte RESTREINT UE/EU RESTRICTED-informationer, som håndteres af kontrahenten, samt retten til at kontrollere de sikkerhedsforanstaltninger, som kontrahenten har truffet. Desuden afleverer kontrahenten en erklæring til den kontraherende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente nationale SAA, som certificerer, at kontrahentens CIS og relaterede sammenkoblinger er akkrediteret til håndtering af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED.

HÅNDTERING AF INFORMATIONER, DER ER KLASSIFICERET RESTREINT UE/EU RESTRICTED, VED HJÆLP AF KOMMUNIKATIONS- OG INFORMATIONSSYSTEMER (CIS)

18. Minimumskravene til CIS, der håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, er fastsat i tillæg E til nærværende SAL.

BETINGELSER HVORPÅ KONTRAHENTEN KAN UDBYDE DELE AF KONTRAKTEN I UNDERENTREPRISE

19. Kontrahenten skal indhente tilladelse fra den berørte Kommissionstjenestegren i dennes kapacitet af kontraherende myndighed, inden en del af en klassificeret kontrakt udbydes i underentreprise.

([4]) Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.

20. En underkontrakt kan ikke tildeles en virksomhed, der er registreret i et tredjeland eller en enhed under en international organisation, hvis det pågældende tredjeland eller den pågældende internationale organisation ikke har indgået en aftale om informationssikkerhed med EU eller en administrativ ordning med Kommissionen.

21. Hvis en kontrahent har tildelt en underkontrakt, finder kontraktens sikkerhedsbestemmelser tilsvarende anvendelse på underkontrahenten og dennes ansatte. I sådanne tilfælde er det kontrahentens ansvar at sikre, at alle underkontrahenter anvender disse bestemmelser på deres egne underentrepriseaftaler. For at sikre passende tilsyn med sikkerheden skal kontrahentens og underkontrahentens NSA/DSA underrettes om tildelingen af relaterede klassificerede underkontrakter med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET. Kontrahentens og underkontrahentens NSA/DSA skal, hvis det er relevant, forelægges en kopi af de kontraktspecifikke sikkerhedskrav for underkontrakten. De NSA'er/DSA'er, der skal underrettes om sikkerhedsbestemmelserne i klassificerede kontrakter med klassifikationsgraden RESTREINT UE/EU RESTRICTED, er opført i bilaget til Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede indkøbskontrakter ([1]).

22. Kontrahenten må ikke videregive EUCI til en underkontrahent uden forudgående skriftlig godkendelse fra den kontraherende myndighed. Hvis EUCI skal sendes til underkontrahenter jævnligt eller rutinemæssigt, kan den kontraherende myndighed give en godkendelse, der gælder for et nærmere fastsat tidsrum (f.eks. 12 måneder), eller så længe underkontrakten gælder.

BESØG

Hvis standardproceduren for besøgsanmodninger skal anvendes på besøg, som indebærer adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal den kontraherende myndighed indarbejde stk. 23, 24 og 25 i kontrakten, men slette stk. 26. Hvis besøg, som indebærer adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, arrangeres direkte mellem den facilitet, der sender den besøgende, og den facilitet, der skal besøges, skal den kontraherende myndighed slette stk. 24 og 25 og kun indarbejde stk. 26 i kontrakten.

23. Besøg, som indebærer adgang eller mulig adgang til informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, arrangeres direkte mellem den facilitet, der sender den besøgende, og den facilitet, der skal besøges, idet det ikke er nødvendigt at følge procedurerne i stk. 24 til 26 nedenfor.

[24. Besøg, som indebærer adgang eller mulig adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, arrangeres efter følgende procedure:

a) Den sikkerhedsansvarlige for den facilitet, der sender den besøgende, udfylder alle relevante dele af besøgsanmodningen (tillæg C) og indgiver den til sin facilitets NSA/DSA.

b) NSA'en/DSA'en for den facilitet, der sender den besøgende, bekræfter den besøgendes PSC, før besøgsanmodningen fremsendes til NSA'en/DSA'en for den facilitet, som skal besøges, (eller til Kommissionens sikkerhedsmyndighed, hvis der er tale om et besøg på Kommissionens lokaliteter).

c) Den sikkerhedsansvarlige for den facilitet, der sender den besøgende, modtager derpå via sin egen NSA/DSA svaret fra NSA'en/DSA'en for den facilitet, som skal besøges, (eller Kommissionens sikkerhedsmyndighed), der enten godkender eller afslår besøgsanmodningen.

d) En besøgsanmodning anses for godkendt, såfremt der ikke foreligger indsigelser senest fem arbejdsdage før dagen for besøget.]

[25. Inden den besøgende gives adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, skal den facilitet, som besøges, have modtaget autorisation fra sin NSA/DSA.]

[26. Besøg, som indebærer adgang eller mulig adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, arrangeres direkte mellem den facilitet, der sender den besøgende, og den facilitet, der skal besøges (tillæg C indeholder et eksempel på den skabelon, der kan anvendes).]

([1]) Den kontraherende myndighed bør indsætte henvisningen hertil, så snart gennemførelsesbestemmelserne er vedtaget.

27. Besøgende skal dokumentere deres identitet ved ankomsten til den facilitet, som besøges, ved fremvisning af gyldigt ID-kort eller pas.

28. Den facilitet, som besøges, skal sikre, at alle besøgende registreres. Denne registrering skal omfatte navn, den organisation, de repræsenterer, udløbsdatoen for PSC'en (hvis relevant), datoen for besøget og navnene på de personer, der besøges. Uden at det berører de europæiske databeskyttelsesregler, opbevares disse oplysninger i mindst tre år eller i overensstemmelse med nationale love og forskrifter, alt efter hvad der er relevant.

VURDERINGSBESØG

29. Kommissionens sikkerhedsmyndighed kan i samarbejde med den relevante NSA/DSA gennemføre besøg på underkontrahenters faciliteter med henblik på at kontrollere, at sikkerhedskravene i forbindelse med håndtering af EUCI er opfyldt.

KLASSIFIKATIONSVEJLEDNING

30. Klassifikationsvejledningen (SCG) indeholder en liste over alle de elementer i kontrakten, der er klassificeret eller skal klassificeres i forbindelse med opfyldelsen af kontrakten, reglerne herfor og specifikationen af den klassifikationsgrad, der skal anvendes. SCG er en integreret del af denne kontrakt og kan findes i tillæg B til dette bilag.

Tillæg B

KLASSIFIKATIONSVEJLEDNING

[den specifikke tekst tilpasses kontraktens genstand]

Tillæg C

BESØGSANMODNING (REQUEST FOR VISIT)

[STANDARDSKABELON]

Detaljeret vejledning til udfyldelse af besøgsanmodningen

(Anmodningen skal indgives på engelsk)

HEADING	Afkrydsningsbokse til type besøg, type informationer og angivelse af, hvor mange steder, der skal besøges, samt antallet af besøgende.
4. **ADMINISTRATIVE DATA**	Udfyldes af den NSA/DSA, der anmoder om besøget.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Angiv fulde navn og postadresse. Hvis det er relevant, angives også by, stat og postnummer.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Angiv fulde navn og postadresse. Angiv også by, stat, postnummer, telex- eller faxnummer (hvis relevant), telefonnummer og e-mail-adresse. Angiv navn og telefonnummer/faxnummer og e-mail-adresse på din primære kontaktperson eller på den person, du har truffet aftalen om besøget med. *Bemærkninger:* 1) Det er vigtigt at angive det korrekte postnummer, eftersom en virksomhed kan have flere forskellige faciliteter. 2) Ved manuelle anmodninger kan bilag 1 anvendes, når to eller flere faciliteter skal besøges i relation til den samme genstand. Når et bilag anvendes, bør punkt 3 udformes således: »SEE ANNEX 1, NUMBER OF FAC: …« (angiv antallet af faciliteter).
7. **DATES OF VISIT**	Angiv den faktiske dato eller periode (dato til dato) for besøget i formatet »dag — måned — år«. Angiv en alternativ dato eller periode i kantede parenteser, hvis det er relevant.
8. **TYPE OF INITIATIVE**	Angiv, hvorvidt den organisation eller facilitet, der anmoder om besøget, har taget initiativ til besøget eller er blevet inviteret af den facilitet, der skal besøges.
9. **THE VISIT RELATES TO:**	Angiv det fulde navn på projektet, kontrakten eller udbuddet. Brug kun almindeligt anvendte forkortelser.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Giv en kort beskrivelse af årsagen til besøget. Brug ikke uforklarede forkortelser. *Bemærkninger:* Hvis der er tale om gentagne besøg, bør »Recurring visits« være de første ord i dataelementet (f.eks. Recurring visits to discuss_____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Skriv SECRET UE/EU SECRET (S-UE/EU-S) eller CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), alt efter hvad der er relevant.
12. **PARTICULARS OF VISITOR**	Bemærkninger: Hvis der er tale om to eller flere besøgende, anvendes bilag 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	Her kræves navn, telefonnummer, faxnummer og e-mail-adresse på den sikkerhedsansvarlige for den facilitet, der anmoder om besøget.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Dette felt udfyldes af den certificerende myndighed. Til den certificerende myndighed: a) Angiv navn, adresse, telefonnummer, faxnummer og e-mail-adresse (kan være fortrykt). b) Dette punkt underskrives og stemples (hvis det er relevant).
15. **REQUESTING SECURITY AUTHORITY**	Dette felt udfyldes af NSA'en/DSA'en. Til NSA'en/DSA'en: a) Angiv navn, adresse, telefonnummer, faxnummer og e-mail-adresse (kan være fortrykt). b) Dette punkt underskrives og stemples (hvis det er relevant).

Alle felter skal udfyldes og anmodningen indgives via de officielle mellemstatslige kanaler ([2]).

([2]) Hvis det er aftalt, at besøg, som indebærer adgang eller mulig adgang til EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, kan arrangeres direkte, kan den udfyldte anmodning indgives direkte til den sikkerhedsansvarlige for den facilitet, som skal besøges.

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Her indsættes referencer til gældende persondatalovgivning og link til obligatoriske oplysninger vedrørende dette emne, f.eks. hvordan artikel 13 i databeskyttelsesforordningen ([3]) gennemføres.>

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

BILAG 1 til besøgsanmodningen

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Her indsættes referencer til gældende persondatalovgivning og link til obligatoriske oplysninger vedrørende dette emne, f.eks. om hvordan artikel 13 i databeskyttelsesforordningen ([1]) gennemføres.>

([1]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

BILAG 2 til besøgsanmodningen

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Her indsættes referencer til gældende persondatalovgivning og link til obligatoriske oplysninger vedrørende dette emne, f.eks. om hvordan artikel 13 i databeskyttelsesforordningen ([1]) gennemføres.>

([1]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

Tillæg D

OPLYSNINGSSKEMA VEDRØRENDE FACILITETSSIKKERHEDSGODKENDELSE (FSC-OPLYSNINGSSKEMA)

[STANDARDSKABELON]

1. **Indledning**

1.1. Vedhæftet et forslag til oplysningsskema vedrørende facilitetssikkerhedsgodkendelse (FSC-oplysningsskema) med henblik på hurtig udveksling af oplysninger mellem den nationale sikkerhedsmyndighed (NSA) eller udpegede sikkerhedsmyndighed (DSA), andre kompetente nationale sikkerhedsmyndigheder og Kommissionen (som kontraherende myndighed) vedrørende facilitetssikkerhedsgodkendelsen af en facilitet, der er berørt af et udbud, en kontrakt eller en underkontrakt.

1.2. FSC-oplysningsskemaet er kun gyldigt, hvis det er stemplet af den relevante NSA/DSA eller en anden kompetent myndiged.

1.3. FSC-oplysningsskemaet er opdelt i to dele, henholdsvis ansøgning om sikkerhedsgodkendelse og svar herpå, og kan anvendes til de formål, der er nævnt ovenfor, eller til andre formål, som kræver, at en facilitet har en sikkerhedsgodkendelse. Begrundelsen for ansøgningen skal angives af den NSA/DSA, der indgiver ansøgningen, i ansøgningens felt nr. 7.

1.4. Oplysningerne på FSC-oplysningsskemaet er normalt ikke klassificerede. Derfor er det at foretrække, at FSC-oplysningsskemaet fremsendes elektronisk mellem de respektive NSA'er/DSA'er/Kommissionen.

1.5. NSA'er/DSA'er bør gøre alt for at besvare en ansøgning om facilitetssikkerhedsgodkendelse inden for ti arbejdsdage.

1.6. Hvis der skal videregives klassificerede informationer eller tildeles en kontrakt i overensstemmelse med en FSC-erklæring, skal den NSA/DSA, der udsteder facilitetssikkerhedsgodkendelsen, underrettes.

PROCEDURER OG VEJLEDNING I ANVENDELSEN AF OPLYSNINGSSKEMAET VEDRØRENDE FACILITETSSIKKERHEDSGODKENDELSE (FSC-OPLYSNINGSSKEMA)

Denne detaljerede vejledning er tiltænkt den NSA/DSA eller Kommissionen som kontraherende myndighed, der udfylder FSC-oplysningsskemaet. Det er at foretrække, at skemaet udfyldes med blokbogstaver.

ADRESSAT	Ansøgeren angiver NSA'ens/DSA'ens fulde navn og landenavn.
1. **TYPE ANSØGNING**	Den kontraherende myndighed, der indgiver ansøgningen, vælger den relevante afkrydsningsboks for den pågældende ansøgning. Her angives også, hvilket sikkerhedsgodkendelsesniveau der ansøges om. Følgende forkortelser bør anvendes: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = kommunikations- og informationssystemer til håndtering af klassificerede informationer

2. **OPLYSNINGER OM FACILITETEN**	Felt nr. 1 til 6 kræver ingen nærmere forklaring. Felt nr. 4 bør udfyldes med landets standardkode på to bogstaver. Felt nr. 5 er frivilligt.
3. **BEGRUNDELSEN FOR ANSØGNINGEN**	Angiv den specifikke årsag til ansøgningen, inklusive projektoplysninger, kontraktnummer eller nummeret på opfordringen til at afgive tilbud. Angiv venligst nærmere oplysninger om lagringskapacitet, CIS-klassifikationsgrad m.m. Alle frister/udløbsdatoer/tildelingsdatoer, der kan have indflydelse for udfærdigelsen af en FSC, bør angives.
4. **NSA/DSA, DER ANSØGER OM EN FSC**	Angiv navnet på den person, der (på vegne af NSA'en/DSA'en) ansøger om FSC'en, og datoen herfor i talformat (dd/mm/åååå).
5. **SVAR PÅ ANSØGNINGEN**	Felt nr. 1-5: Vælg de relevante felter. Felt nr. 2: Hvis en FSC-ansøgning er under behandling, anbefales det at meddele ansøgeren en forventet behandlingstid (såfremt denne kendes). Felt nr. 6: a) Selv om valideringen kan variere fra land til land og endda fra facilitet til facilitet, anbefales det at angive en udløbsdato for FSC'en. b) I tilfælde hvor FSC-erklæringen ikke har en udløbsdato, kan dette felt streges ud. c) Ansøgeren, kontrahenten eller underkontrahenten er ansvarlig for at ansøge om fornyelse af FSC'en, jf. de respektive nationale love og forskrifter.
6. **BEMÆRKNINGER**	Kan bruges til at angive yderligere oplysninger om FSC'en, faciliteten eller oplysninger afgivet ovenfor.
7. **NSA/DSA, DER UDSTEDER FSC'EN**	Angiv navnet på den myndighed, der (på vegne af NSA'en/DSA'en) udsteder FSC'en, og datoen herfor i talformat (dd/mm/åååå).

OPLYSNINGSSKEMA VEDRØRENDE FACILITETSSIKKERHEDSGODKENDELSE (FSC-OPLYSNINGSSKEMA)

[STANDARDSKABELON]

Alle felter skal udfyldes og skemaet indgives via de officielle mellemstatslige kanaler eller diplomatiet mellem stater og internationale organisationer.

ANSØGNING OM FACILITETSSIKKERHEDSGODKENDELSESERKLÆRING

TIL: _____

(NSA/DSA landenavn)

Afkryds venligst de relevante bokse:

[ ] Udstedelse af en FSC-erklæring på følgende niveau: [ ] S-UE/EU-S [ ] C-UE/EU-C

til nedenstående facilitet

[ ] Inklusive sikker opbevaring af EU-klassificeret materiale/EU-klassificerede informationer

[ ] Inklusive kommunikations- og informationssystemer (CIS) til håndtering af klassificerede informationer

[ ] Indledning, på direkte anmodning eller på tilsvarende anmodning af en kontrahent eller underkontrahent, af proceduren for opnåelse af en FSC op til og inklusive niveau ..... med .....-niveau for sikker opbevaring og .....-niveau for CIS, hvis faciliteten på nuværende tidspunkt ikke har denne kapacitet.

Bekræft nøjagtigheden af oplysningerne om de nedenfor angivne faciliteter og angiv eventuelle rettelser/tilføjelser.

1. Facilitetens fulde navn:	Rettelser/tilføjelser:
.....	.....
2. Facilitetens fulde adresse	
.....	.....
3. Postadresse (hvis forskellig fra 2)	
.....	.....
4. Postnummer/by/land	
.....	.....
5. Navn på den sikkerhedsansvarlige	
.....	.....
6. Telefonnummer/Faxnummer/E-mail-adresse på den sikkerhedsansvarlige	
.....	.....

7. Denne ansøgning indgives af følgende årsager: (angiv oplysninger om fasen forud for kontraktens indgåelse (udvælgelse af forslag), kontrakten eller underkontrakten, programmet/projektet osv.)

.....

NSA/DSA/Kommissionen som kontraherende myndighed, der indgiver ansøgningen: Navn: ..... Dato: (dd/mm/åååå) .....

SVAR (inden for ti arbejdsdage)

Det certificeres herved, at

1. [ ] ovennævnte facilitet har en FSC op til og inklusive følgende niveau [ ] S-UE/EU-S

   [ ] C-UE/EU-C

2. ovennævnte facilitet har kapacitet til sikker opbevaring af klassificerede informationer/klassificeret materiale

   [ ] ja, niveau: ..... [ ] nej

3. ovennævnte facilitet har et akkrediteret/autoriseret CIS:

   [ ] ja, niveau: ..... [ ] nej

4. [ ] der i forbindelse med ovennævnte ansøgning er indledt en procedure for opnåelse af FSC. De underrettes, når FSC'en er blevet givet eller afvist.

5. [ ] ovennævnte facilitet ikke har en FSC.

6. FSC-erklæringen udløber den: ..... (*dd/mm/åååå*), eller som anbefalet af NSA'en/DSA'en. Hvis FSC'en udløber tidligere, eller der sker ændringer i ovennævnte, underrettes De herom.

7. Bemærkninger:

   .....

NSA/DSA, der udsteder FSC'en *Navn:* ..... *Dato: (dd/mm/åååå)* .....

<Her indsættes referencer til gældende persondatalovgivning og link til obligatoriske oplysninger vedrørende dette emne, f.eks. om hvordan artikel 13 i databeskyttelsesforordningen ([2]) gennemføres.>

([2]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

Tillæg E

Minimumskrav til sikkerhedsbeskyttelse af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED i elektronisk form, der håndteres af kontrahentens CIS

Generelt

1. Kontrahenten er ansvarlig for at sikre, at sikkerhedsbeskyttelsen af RESTREINT UE/EU RESTRICTED-informationer overholder de minimumssikkerhedskrav, der er fastsat i sikkerhedsklausulen, og alle andre yderligere krav anbefalet af den kontraherende myndighed eller, hvis det relevant, den nationale sikkerhedsmyndighed (NSA) eller den udpegede sikkerhedsmyndighed (DSA).

2. Det er kontrahentens ansvar at gennemføre de sikkerhedskrav, der er angivet i dette dokument.

3. I dette dokument forstås ved kommunikations- og informationssystem (CIS) alt udstyr til håndtering, lagring og transmission af EUCI, herunder arbejdsstationer, printere, kopimaskiner, faxmaskiner, servere, netværksdriftssystemer, netværkskontrolsystemer og kommunikationskontrolsystemer, bærbare computere, tabletcomputere, smartphones og transportable lagringsenheder, såsom USB-nøgler, CD'er, SD-kort m.m.

4. Særligt udstyr, såsom kryptoprodukter, skal beskyttes i overensstemmelse med de særlige operationelle sikkerhedsprocedurer (SecOP).

5. Kontrahenter skal etablere en struktur, der er ansvarlig for sikkerhedsstyringen af det CIS, som håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, og som udpeger en sikkerhedsansvarlig for den berørte facilitet.

6. IT-løsninger (hardware, software eller tjenester), der ejes privat af kontrahentens ansatte, må ikke anvendes til lagring eller behandling af RESTREINT UE/EU RESTRICTED-informationer.

7. Akkreditering af kontrahentens CIS, som håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal godkendes af sikkerhedsakkrediteringsmyndigheden (SAA) i den relevante medlemsstat eller uddelegeres til kontrahentens sikkerhedsansvarlige, såfremt dette er tilladt i henhold til nationale love og forskrifter.

8. Informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, må kun håndteres, lagres eller transmitteres (ved hjælp af trådbunden eller trådløs forbindelse) på samme måde som ikkeklassificerede informationer i forbindelse med kontrakten, hvis de er krypteret ved hjælp af godkendte kryptoprodukter. Sådanne kryptoprodukter skal være godkendt af EU eller af en medlemsstat.

9. Eksterne faciliteter, som er involveret i vedligeholdelse/reparation, skal være kontraktligt forpligtede til at overholde de gældende bestemmelser for håndtering af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, som fastsat i dette dokument.

10. På anmodning af den kontraherende myndighed eller den relevante NSA/DSA/SAA skal kontrahenten dokumentere overholdelse af kontraktsikkerhedsklausulen. Hvis der også anmodes om en revision og kontrol af kontrahentens procedurer og faciliteter med henblik på at sikre overholdelse af kravene, skal kontrahenten give repræsentanter for den kontraherende myndighed, NSA'en/DSA'en/SAA'en eller den relevante EU-sikkerhedsmyndighed adgang til at gennemføre en sådan revision og kontrol.

Fysisk sikkerhed

11. Områder, hvor CIS anvendes til at vise, lagre eller transmittere RESTREINT UE/EU RESTRICTED-informationer, eller områder, der huser servere, netværksdriftssystemer, netværkskontrolsystemer og kommunikationskontrolsystemer til sådanne CIS, bør etableres som separate og kontrollerede områder med et hensigtsmæssigt adgangskontrolsystem. Adgangen til disse separate og kontrollerede områder bør begrænses til personer med en specifik autorisation. Uden at det berører stk. 8, skal udstyr som beskrevet i stk. 3, opbevares i sådanne separate og kontrollerede områder.

12. Der skal gennemføres sikkerhedsmekanismer og/eller -procedurer med henblik på at regulere indføringen eller tilslutningen af en bærbar computerlagringsenhed (såsom USB-nøgler, masselagringsenheder eller CD-RW'er) i/til dele af CIS'et.

Adgang til CIS

13. Adgang til en kontrahents CIS, der håndterer EUCI, kan kun gives på grundlag af need to know og til autoriserede ansatte.

14. Der skal foreligge en ajourført liste over autoriserede brugere for alle CIS. Alle brugere skal autentificeres ved begyndelsen af hver behandlingssession.

15. Adgangskoder, som er en del af de fleste sikkerhedsidentifikations- og sikkerhedsautentifikationsforanstaltninger, skal have en længde på minimum ni karakterer og indeholde numeriske tegn og specialtegn (hvis systemet tillader det) samt alfabetiske tegn. Adgangskoder skal skiftes mindst hver 180. dag. Hvis de er blevet kompromitteret eller afsløret over for en uautoriseret person, eller hvis der er mistanke om en sådan kompromittering eller afsløring, skal de ændres så hurtigt som muligt.

16. Alle CIS skal være udstyret med intern adgangskontrol for at forhindre, at uautoriserede brugere får adgang til eller ændrer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, eller ændrer systemet og sikkerhedskontrollerne. Brugere skal automatisk logges af det pågældende CIS, hvis deres terminaler har været inaktive i en nærmere fastsat tidsperiode. Alternativt skal CIS aktivere en pauseskærm, der er beskyttet med adgangskode, efter 15 minutters inaktivitet.

17. Hver bruger af det pågældende CIS tildeles en unik brugerkonto og et unikt brugerid. Brugerkontoen skal låse automatisk efter fem fejlslagne forsøg på at logge på i træk.

18. Alle brugere af CIS skal gøres opmærksom på deres ansvar og de procedurer, der skal følges for at beskytte informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, og som ligger i CIS. Ansvaret og de procedurer der skal følges, skal dokumenteres og brugerne skal skriftlig anerkende dem.

19. SecOP'erne skal være tilgængelige for brugerne og administratorerne og skal omfatte beskrivelser af sikkerhedsrollerne og de dertil knyttede lister over opgaver instrukser og planer.

Registrering, revision og beredskab

20. Enhver adgang til CIS skal logges.

21. Følgende hændelser skal registreres:

    a) alle forsøg på at logge på, uanset om det lykkes eller ej

    b) hver gang der logges af (inklusive når der logges af automatisk, hvis det er relevant)

    c) oprettelse, sletning og ændring af adgangsrettigheder og -privilegier

    d) oprettelse, sletning og ændring af adgangskoder.

22. I forbindelse med de hændelser, der er anført nedenfor, skal følgende oplysninger som minimum kommunikeres:

    a) type hændelse

    b) brugerid

    c) dato og tidspunkt

    d) udstyrets idnummer.

23. Registreringerne skal kunne hjælpe den sikkerhedsansvarlige i forbindelse med undersøgelser af potentielle sikkerhedshændelser. De kan også anvendes til at understøtte eventuelle retlige undersøgelser i forbindelse med en sikkerhedshændelse. Alle sikkerhedsregistreringer skal kontrolleres regelmæssigt med henblik på at opdage potentielle sikkerhedshændelser. Registreringerne skal beskyttes mod uautoriseret sletning eller ændring.

24. Kontrahenten skal have en etableret beredskabsstrategi med henblik på håndtering af sikkerhedshændelser. Brugere og administratorer skal instrueres i, hvordan de skal reagere på hændelser, hvordan de skal indberette dem, og hvad de skal gøre i et nødstilfælde.

25. Kompromittering eller mistanke om kompromittering af informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal indberettes til den kontraherende myndighed. Indberetningen skal omfatte en beskrivelse af de informationer, der er berørt, og en beskrivelse af omstændighederne omkring kompromitteringen eller mistanken herom. Alle brugere af CIS skal gøres opmærksom på, hvordan de indberetter en faktisk sikkerhedshændelse eller en mistanke herom til den sikkerhedsansvarlige.

Netværk og sammenkobling

26. Når en kontrahents CIS, som håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, er koblet sammen med et CIS, der ikke er akkrediteret, øger det væsentligt truslen mod CIS sikkerhed og sikkerhedsbeskyttelsen af de RESTREINT UE/EU RESTRICTED-informationer, der håndteres af CIS. Dette omfatter internettet og andre offentlige eller private CIS, såsom andre CIS, der ejes af kontrahenten eller underkontrahenten. Hvis dette er tilfældet, skal kontrahenten foretage en risikovurdering med henblik på at udpege yderligere sikkerhedskrav, der skal opfyldes i forbindelse med sikkerhedsakkrediteringsprocessen. Kontrahenten skal aflevere en erklæring til den kontraherende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente SAA, som certificerer, at kontrahentens CIS og relaterede sammenkoblinger er akkrediteret til håndtering af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED.

27. Fjernadgang fra andre systemer til LAN-tjenester (f.eks. fjernadgang til e-mail-systemer og fjernsupport af systemer) er forbudt, medmindre der gennemføres særlige sikkerhedsforanstaltninger, som er aftalt med den kontraherende myndighed, og, såfremt det kræves i henhold til nationale love og forskrifter, er godkendt af den kompetente SAA.

Konfigurationsstyring

28. Der skal være en detaljeret hardware- og softwarekonfiguration tilgængelig, jf. akkrediterings-/godkendelsesdokumentationen (herunder system- og netværksdiagrammer), som vedligeholdes regelmæssigt.

29. Kontrahentens sikkerhedsansvarlige skal udføre konfigurationskontrol på såvel hardware som software for at sikre, at der ikke anvendes uautoriseret hardware eller software.

30. Ændringer i kontrahentens CIS-konfiguration skal vurderes med henblik på sikkerheden og godkendes af den sikkerhedsansvarlige og, såfremt det kræves i henhold til nationale love og forskrifter, SAA'en.

31. Systemet skal scannes for sårbarheder, der påvirker sikkerheden, mindst en gang i kvartalet. Software til afsløring af malware skal installeres og holdes opdateret. Hvis det er muligt, skal sådan software have en national eller internationalt anerkendt godkendelse. Alternativt skal den opfylde almindeligt accepterede industristandarder.

32. Kontrahenten skal udarbejde en kontinuitetsplan. Der skal etableres backupprocedurer med henblik på at fastsætte følgende:

a) hvor ofte der tages backup

b) opbevaringskrav på stedet (brandsikre containere) og uden for stedet

c) kontrol af autoriseret adgang til backupkopier.

Rensning og destruktion

33. CIS eller datalagringsmedier, der på et eller andet tidspunkt har lagret RESTREINT UE/EU RESTRICTED-informationer, skal underkastes følgende resning af hele systemet eller lagringsmediet, før det kasseres:

a) flashhukommelser (f.eks. USB-nøgler, SD-kort, drev (SSD), hybride harddiske (HHD)) skal overskrives mindst tre gange og derpå verificeres for at sikre, at det originale indhold ikke kan genskabes eller slettes ved hjælp af godkendt sletningssoftware

b) magnetiske medier (f.eks. harddiske) skal overskrives eller afmagnetiseres

c) optiske medier (f.eks. CD'er og DVD'er) skal makuleres eller disintegreres

d) den kontraherende myndighed eller, hvis det er relevant, NSA/DSA/SAA skal konsulteres om de sikkerhedskrav, der skal opfyldes i forbindelse med alle andre typer lagringsmedier.

34. Et lagringsmedie, som lagrer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal renses, før det overdrages til en enhed, der ikke er autoriseret til at få adgang til informationer, der er klassificeret RESTREINT UE/EU RESTRICTED (f.eks. med henblik på vedligeholdelse).

BILAG IV

Facilitets- og personelsikkerhedsgodkendelse til kontrahenter, som omfatter adgang til RESTREINT UE/EU RESTRICTED-informationer, og NSA'er/DSA'er, der kræver underretning om klassificerede kontrakter med klassifikationsgraden RESTREINT UE/EU RESTRICTED ([1])

Medlemsstat	FSC		Underretning om kontrakter eller underkontrakter, der omfatter adgang til R-UE/EU-R-informationer, til NSA'en/DSA'en		PSC	
	JA	NEJ	JA	NEJ	JA	NEJ
Belgien		X		X		X
Bulgarien		X		X		X
Tjekkiet		X		X		X
Danmark	X		X		X	
Tyskland		X		X		X
Estland	X		X			X
Irland		X		X		X
Grækenland	X			X	X	
Spanien		X	X			X
Frankrig		X		X		X
Kroatien		X	X			X
Italien		X	X			X
Cypern		X	X			X
Letland		X		X		X

([1]) Disse nationale krav vedrørende FSC/PSC og underretning om kontrakter, der indebærer adgang til RESTREINT UE/EU RESTRICTED-informationer, må ikke medføre yderligere forpligtelser for andre medlemsstater eller kontrahenter under deres jurisdiktion.
NB Underretninger om kontrakter, der indebærer adgang til CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET-informationer, er obligatoriske.

Medlemsstat	FSC		Underretning om kontrakter eller underkontrakter, der omfatter adgang til R-UE/EU-R-informationer, til NSA'en/DSA'en		PSC	
	JA	NEJ	JA	NEJ	JA	NEJ
Litauen	X		X			X
Luxembourg	X		X		X	
Ungarn		X		X		X
Malta		X		X		X
Nederlandene	X (kun kontrakter, der vedrører forsvar)		X (kun kontrakter, der vedrører forsvar)			X
Østrig		X		X		X
Polen		X		X		X
Portugal		X		X		X
Rumænien		X		X		X
Slovenien	X		X			X
Slovakiet	X		X			X
Finland		X		X		X
Sverige	X (kun kontrakter, der vedrører forsvar)		X (kun kontrakter, der vedrører forsvar)		X (kun kontrakter, der vedrører forsvar)	
Det Forenede Kongerige		X		X		X

BILAG V

LISTE OVER NATIONALE SIKKERHEDSMYNDIGHEDER/AFDELINGER I UDPEGEDE SIKKERHEDSMYNDIGHEDER MED ANSVAR FOR PROCEDURER VEDRØRENDE INDUSTRISIKKERHED

BELGIEN

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tlf. +32 25014542 (Secretariat)
Fax +32 25014596
Email: nvo-ans@diplobel.fed.be

BULGARIEN

1. State Commission on Information Security — National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tlf. +359 29835775
   Fax +359 29873750
   Email: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tlf. +359 29227002
   Fax +359 29885211
   Email: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tlf. +359 29813221
   Fax +359 29862706
   Email: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tlf. +359 29824971
   Fax +359 29461339
   Email: dato@dato.bg

   (De kompetente myndigheder, der er anført ovenfor, gennemfører screeningsprocedurer med henblik på udstedelse af FSC til juridiske enheder, der ansøger om indgåelse af en klassificeret kontrakt, og PSC til enkeltpersoner, der gennemfører en klassificeret kontrakt på vegne af disse myndigheder.)

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tlf. +359 28147109
   Fax +359 29632188, +359 28147441
   Email: dans@dans.bg

   (De sikkerhedstjenester, der er anført ovenfor, gennemfører screeningsprocedurer med henblik på udstedelse af FSC og PSC til alle andre juridiske enheder og enkeltpersoner i landet, som ansøger om indgåelse af en klassificeret kontrakt eller gennemførelse en klassificeret kontrakt.)

TJEKKIET

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tlf. +420 257283129
Email: sbr@nbu.cz

DANMARK

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

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

TYSKLAND

1. Spørgsmål vedrørende industrisikkerhedspolitik, FSC og transportplaner (med undtagelse af krypto-/fortrolige forretningsoplysninger):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division — ZB3
Villemombler Str. 76
53123 Bonn
Tlf. +49 228996154028
Fax +49 228996152676
Email: dsagermany-zb3@bmwi.bund.de (office email address)

2. Standardbesøgsanmodninger fra/i tyske virksomheder:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division — ZB2
Villemombler Str. 76
53123 Bonn
Tlf. +49 228996152401
Fax +49 228996152603
Email: zb2-international@bmwi.bund.de (office email address)

3. Transportplaner vedrørende kryptomateriale:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tlf. +49 2289995826052
Fax +49 228991095826052
Email: NDAEU@bsi.bund.de

ESTLAND

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tlf. +372 6939211
Fax +372 6935001
Email: nsa@fis.gov.ee

IRLAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tlf. +353 14082724
Email: nsa@dfa.ie

GRÆKENLAND

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Tlf. +30 2106572022, +30 2106572178
Fax +30 2106527612
Email: daa.industrial@hndgs.mil.gr

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tlf. +34 913725000
Fax +34 913725808
Email: nsa-sp@areatec.com
Personelsikkerhedsgodkendelser: asip@areatec.com
Transportplaner og internationale besøg: sp-ivtco@areatec.com

FRANKRIG

National Security Authority (NSA) (politik og gennemførelse på andre områder end forsvarsindustri)
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
Tlf. +33 171758193
Fax +33 171758200
Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (gennemførelse på området for forsvarsindustri)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15
Tlf. +33 988670421
Email: skemaer og udgående besøgsanmodninger: dga-ssdi.ai.fct@intradef.gouv.fr
indkommende besøgsanmodninger: dga-ssdi.visit.fct@intradef.gouv.fr

KROATIEN

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tlf. +385 14681222
Fax +385 14686049
Email: NSACroatia@uvns.hr

ITALIEN

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

CYPERN

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
Email: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Tlf. +357 22807569, +357 22807764
Fax +357 22302351
Email: cynsa@mod.gov.cy

LETLAND

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tlf. +371 67025418, +371 67025463
Fax +371 67025454
Email: ndi@sab.gov.lt, ndi@zd.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
Tlf. +370 70666703, +370 70666701
Fax +370 70666700
Email: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tlf. +352 24782210
Email: ans@me.etat.lu

UNGARN

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tlf. +36 13911862
Fax +36 13911889
Email: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Fax +356 21242406
Email: certification@mccaa.org.mt

NEDERLANDENE

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tlf. +31 703204400
Fax +31 703200733
Email: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tlf. +31 704419407
Fax +31 703459189
Email: indussec@mindef.nl

ØSTRIG

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Tlf. +43 153115202594
Email: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
Email: abwa@bmlvs.gv.at

POLEN

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Tlf. +48 225857944
Fax +48 225857443
Email: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tlf. +351 213031710
Fax +351 213031711
Email: sind@gns.gov.pt, franco@gns.gov.pt

RUMÆNIEN

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS
Romanian NSA — ORNISS — National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tlf. +40 212075115
Fax +40 212245830
Email: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tlf. +386 14781390
Fax +386 14781399
Email: gp.uvtp@gov.si

SLOVAKIET

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tlf. +421 268691111
Fax +421 268691700
Email: podatelna@nbu.gov.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Email: NSA@formin.fi

SVERIGE

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tlf. +46 84051000
   Fax +46 87231176
   Email: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tlf. +46 87824000
   Fax +46 87826900
   Email: security@fmv.se

DET FORENEDE KONGERIGE

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tlf. +44 2072765497, +44 2072765645
Email: UK-NSA@cabinet-office.x.gsi.gov.uk