KOMMISSIONENS AFGØRELSE (EU, Euratom) 2021/259

af 10. februar 2021

om gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede tilskud

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 Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget og 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 ([1]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen ([2]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer ([3]),

under henvisning til Kommissionens afgørelse (EU, Euratom) 2017/46 af 10. januar 2017 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen ([4]), og

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

ud fra følgende betragtninger:

(1) Det fremgår af artikel 41, 42, 47 og 48 i afgørelse (EU, Euratom) 2015/444, at der med henblik på at supplere og fremme gennemførelse af afgørelsens kapitel 6 skal fastsættes gennemførelsesbestemmelser om industrisikkerhed, der bl.a. omfatter tildeling af klassificerede tilskudsaftaler, facilitetssikkerhedsgodkendelser, personelsikkerhedsgodkendelser, besøg og transmission og transport af EU's klassificerede informationer (»EUCI«).

(2) Det fremgår af afgørelse (EU, Euratom) 2015/444, at klassificerede tilskudsaftaler skal gennemføres i tæt samarbejde med den nationale sikkerhedsmyndighed, den udpegede sikkerhedsmyndighed eller en anden kompetent myndighed i de pågældende medlemsstater. Medlemsstaterne er enige om at sikre, at enhver enhed under deres jurisdiktion, som vil kunne modtage eller udarbejde klassificerede informationer udstedt af Kommissionen, er behørigt sikkerhedsgodkendt og kan yde passende beskyttelse, der er 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 som nævnt i aftalen mellem Den Europæiske Unions medlemsstater, forsamlet i Rådet, om beskyttelse af klassificerede informationer, der udveksles i Den Europæiske Unions interesse (2011/C 202/05) ([5]).

([1]) EUT L 193 af 30.7.2018, s. 1.
([2]) EUT L 72 af 17.3.2015, s. 41.
([3]) EUT L 72 af 17.3.2015, s. 53.
([4]) EUT L 6 af 11.1.2017, s. 40.
([5]) EUT C 202 af 8.7.2011, s. 13.

(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 ([6]) blev vedtaget.

(4) Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede tilskud bør derfor også sikre størst mulig overensstemmelse og tage hensyn til retningslinjerne for industrisikkerhed godkendt af Rådets Sikkerhedsudvalg den 13. december 2016.

(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 —

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 tilskud i overensstemmelse med afgørelse (EU, Euratom) 2015/444, særlig kapitel 6 deri.

2. I denne afgørelse fastsættes specifikke krav til sikkerhedsbeskyttelse af EU-klassificerede informationer (EUCI) i offentliggørelsen af indkaldelser, og ved tildeling af tilskud og gennemførelse af klassificerede tilskudsaftaler indgået af Europa-Kommissionen.

3. Denne afgørelse finder anvendelse på tilskud, som vedrører informationer med følgende klassifikationsgrader:

a) RESTREINT UE/EU RESTRICTED

b) CONFIDENTIEL UE/EU CONFIDENTIAL

c) SECRET UE/EU SECRET.

4. Denne afgørelse finder anvendelse, uden at det berører specifikke regler fastlagt i andre retsakter, som dem vedrørende programmet for udvikling af den europæiske forsvarsindustri.

Artikel 2

Kommissionens ansvar

1. Som en del af den tilskudsgivende myndigheds anvisningsberettigedes ansvar, jf. Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046, skal den pågældende anvisningsberettigede sikre, at det klassificerede tilskud følger afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil.

([6]) 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).

([7]) Kommissionens afgørelse af 4.5.2016 om bemyndigelse vedrørende sikkerhed (COM(2016) 2797 final).

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

3. Når program- eller projektsikkerhedsinstruktioner, jf. artikel 5, stk. 3, finder anvendelse, udøver den tilskudsgivende myndighed og Kommissionens sikkerhedsmyndighed de beføjelser, der er tildelt dem i disse instruktioner.

4. 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.

5. Når tilskud forvaltes af EU's forvaltningsorganer eller andre finansieringsorganer, og de specifikke regler fastlagt i andre retsakter, jf. artikel 1, stk. 4, ikke finder anvendelse:

a) skal de rettigheder, udstederen har, udøves af Kommissionens delegerede tjenestegrene for så vidt angår EUCI, der udarbejdes i forbindelse med tilskuddene, for så vidt delegeringsaftalen foreskriver dette

b) er Kommissionens delegerede tjenestegrene ansvarlige for at fastlægge klassifikationsgraden

c) skal anmodninger om informationer om sikkerhedsgodkendelser og underretningerne af NSA'er og/eller DSA'er fremsendes via Kommissionens sikkerhedsmyndighed.

KAPITEL 2

HÅNDTERING AF UDBUD VEDRØRENDE KLASSIFICEREDE TILSKUD

Artikel 3

Grundprincipper

1. Klassificerede dele af tilskuddene gennemføres udelukkende af tilskudsmodtagere, som er registreret i en medlemsstat, eller tilskudsmodtagere, 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 Unionen eller en administrativ ordning med Kommissionen ([8]).

2. Inden der iværksættes et udbud om indgåelse af et klassificeret tilskud, fastsætter den tilskudsgivende myndighed klassifikationsgraden for de informationer, som måtte blive videregivet til ansøgerne. Den tilskudsgivende myndighed fastsætter også den højeste klassifikationsgrad for informationer, som frembringes i forbindelse med opfyldelsen af tilskudsaftalen, 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).

3. Den tilskudsgivende myndighed sikrer, at udbudsbekendtgørelser vedrørende klassificerede tilskud omfatter oplysninger om de særlige sikkerhedsmæssige forpligtelser, der skal opfyldes i forbindelse med klassificerede informationer. Udbudsdokumenterne skal indeholde præciseringer af tidslinjen for tilskudsmodtageres indhentelse af FSC'er, når det kræves. Bilag I og II indeholder forslag til skabeloner til oplysningerne vedrørende udbudsbetingelserne.

([8]) 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.

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

5. Hvis RESTREINT UE/EU RESTRICTED-informationer skal videregives til ansøgere, indarbejdes minimumskravene i artikel 5, stk. 7, i nærværende afgørelse i udbuddet eller i de fortrolighedsaftaler, der indgås i forslagsfasen.

6. Alle ansøgere og tilskudsmodtagere, som skal håndtere eller lagre informationer klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET på deres faciliteter, enten i forbindelse med forslagsfasen eller i forbindelse med opfyldelsen af den klassificerede tilskudsaftale, skal være i besiddelse af en FSC på det krævede niveau, undtagen i de i stk. 9 nævnte tilfælde. Følgende beskriver de tre scenarier, der kan opstå i forbindelse med forslagsfasen for et klassificeret tilskud, som omfatter EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET:

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

   Hvis udbuddet vedrører et tilskud, som vil indebære adgang til EUCI med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, men som ikke kræver, at ansøgeren håndterer sådanne informationer i forslagsfasen, må en ansøger, der ikke er i besiddelse af en FSC på det krævede niveau, ikke udelukkes fra ansøgningsproceduren 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 forslagsfasen på den tilskudsgivende myndigheds lokaliteter:

   Der gives adgang til de af ansøgers ansatte, der er i besiddelse af en PSC på det krævede niveau, hvis de har et need to know.

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

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

7. I princippet bør der ikke kræves en FSC eller PSC for at få adgang til RESTREINT UE/EU RESTRICTED-informationer, hverken i forslagsfasen eller i forbindelse med opfyldelse af tilskudsaftalen. Hvis en medlemsstat kræver en FSC eller PSC i forbindelse med tilskudsaftaler 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 ansøgere, tilskudsmodtagere eller underkontrahenter fra medlemsstater, som ikke stiller sådanne FSC- eller PSC-krav for adgang til RESTREINT UE/EU RESTRICTED-informationer, i forbindelse med relaterede tilskudsaftaler eller underkontrakter eller en udbudsprocedure vedrørende sådanne. Sådanne kontrakter opfyldes i medlemsstaterne i henhold til de nationale love og forskrifter.

8. Hvis der kræves en FSC til håndtering af et udbud og opfyldelse af en klassificeret tilskudsaftale, fremsender den tilskudsgivende myndighed, gennem Kommissionens sikkerhedsmyndighed, en anmodning til tilskudsmodtagerens NSA eller DSA i form af et FSC-oplysningsskema eller tilsvarende i elektronisk form. Bilag III, tillæg D, indeholder et eksempel på et FSC-oplysningsskema ([9]). Der gives så vidt muligt svar på fremsendelsen af et FSC-oplysningsskema inden for ti arbejdsdage fra anmodningsdatoen.

9. Hvis en medlemsstats regeringsinstitutioner eller institutioner, der er under tilsyn af deres regering, deltager i klassificerede tilskud, som kræver FSC'er, og hvis FSC'er ikke udstedes for disse institutioner i henhold til medlemsstatens nationale love, verificerer den tilskudsgivende myndighed, gennem Kommissionens sikkerhedsmyndighed, hos den pågældende NSA eller DSA, om disse regeringsinstitutioner kan håndtere EUCI på det krævede niveau.

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

10. Hvis der kræves en PSC til opfyldelse af en klassificeret tilskudsaftale, og hvis en FSC i henhold til de nationale regler er nødvendig, før en PSC tildeles, forhører den tilskudsgivende myndighed sig hos tilskudsmodtagerens NSA eller DSA, gennem Kommissionens sikkerhedsmyndighed, i form af et FSC-oplysningsskema, om tilskudsmodtageren er i besiddelse af en FSC, eller om FSC-processen er i gang. Her fremsætter Kommissionen ikke anmodninger om PSC'er, i form af et PSC-oplysningsskema.

Artikel 4

Underentreprise i forbindelse med klassificerede tilskud

1. De betingelser, hvorpå tilskudsmodtagere kan udbyde i projektopgaver i underentreprise, som omfatter EUCI, fastsættes i udbuddet og i tilskudsaftalen. Nævnte betingelser skal sikre, at alle FSC-oplysningsskemaer fremsendes gennem Kommissionens sikkerhedsmyndighed. Underentreprise kræver, at den tilskudsgivende myndighed forud herfor giver skriftligt samtykke hertil. Underentrepriser skal efterkomme den grundlæggende retsakt om programmets oprettelse, hvis det er relevant.

2. Klassificerede dele af tilskuddene udbydes udelukkende i underentreprise til enheder, som er registreret i en medlemsstat, eller enheder, 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 Unionen eller en administrativ ordning med Kommissionen ([10]).

KAPITEL 3

HÅNDTERING AF KLASSIFICEREDE TILSKUD

Artikel 5

Grundprincipper

1. Ved tildelingen af et klassificeret tilskud sikrer den tilskudsgivende myndighed sammen med Kommissionens sikkerhedsmyndighed, at tilskudsmodtagernes forpligtelser for så vidt angår sikkerhedsbeskyttelse af EUCI, der anvendes eller frembringes i forbindelse med opfyldelse af tilskudsaftalen er indarbejdet i tilskudsaftalen. Tilskudsspecifikke sikkerhedskrav fremgår af de særlige sikkerhedsbetingelser (SAL). Bilag III indeholder et forslag til en SAL-skabelon.

2. Inden den tilskudsgivende myndighed underskriver et klassificeret tilskud, godkender den en klassifikationsvejledning (SCG) med henblik på de opgaver, der skal udføres, og de informationer, der frembringes i forbindelse med opfyldelsen af tilskuddet, 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 tilskudsaftale er en del af et program eller et projekt, der har sin egen PSI, udarbejdes tilskudsaftalens SAL i forenklet form med en henvisning til sikkerhedsbestemmelserne i programmets eller projektets PSI.

4. Undtagen i de i artikel 3, stk. 9, nævnte tilfælde underskrives den klassificerede tilskudsaftale først, når ansøgerens NSA eller DSA har bekræftet, at ansøgeren er i besiddelse af en FSC, eller, hvis den klassificerede tilskudsaftale tildeles et konsortium, først når mindst én ansøgers NSA eller DSA, inden for konsortiet, eller flere om nødvendigt, har bekræftet, at ansøgeren er i besiddelse af en FSC.

5. I princippet, og medmindre andet er fastsat i andre relevante regler, anses den tilskudsgivende myndighed for at være udstederen af EUCI, der frembringes i forbindelse med opfyldelsen af tilskudsaftalen.

([10]) 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.

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

7. Tilskudsaftaler, som omfatter informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal indeholde en sikkerhedsklausul, der gør bestemmelserne i bilag III, tillæg E, bindende for tilskudsmodtagerne. 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 tilskudsmodtagere, til akkreditering af deres CIS, der håndterer RESTREINT UE/EU RESTRICTED-informationer.

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

Artikel 6

Tilskudsmodtagerens og underkontrahentens ansattes adgang til EUCI

1. Den tilskudsgivende myndighed sikrer, at klassificerede tilskudsaftaler indeholder bestemmelser om, at en tilskudsmodtagers eller underkontrahents ansatte, der med henblik på opfyldelsen af den klassificerede tilskudsaftale eller underentreprisekontrakt har behov for adgang til EUCI, kun indrømmes adgang, hvis:

a) det er fastslået, at de har 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 eller 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. Adgang til EUCI skal også ske i overensstemmelse med den grundlæggende retsakt om programmets oprettelse og under hensyntagen til yderligere mærkninger, som defineret i SCG'en, hvis det er relevant.

3. Hvis en tilskudsmodtager 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 tilskudsmodtagerens 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.

Artikel 7

Adgang til EUCI for eksperter, der deltager i kontrol, gennemgang eller revision

1. Hvis eksterne deltagere (eksperter) er involverede i kontrol, gennemgang eller revision foretaget af den tilskudsgivende myndigheder eller i performancevurderinger af tilskudsmodtagere, som skal have adgang til informationer, der er klassificeret CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET, tildeles de kun en kontrakt, hvis de har en PSC på det relevante niveau udstedt af deres respektive NSA eller DSA eller en anden kompetent sikkerhedsmyndigheder. Den tilskudsgivende myndighed undersøger og anmoder, hvis det er relevant, via Kommissionens sikkerhedsmyndighed, NSA'en eller DSA'en om at indlede screeningsprocedurer med henblik på eksperter mindst seks måneder før, deres respektive kontrakter træder i kraft.

2. Inden eksperterne underskriver deres kontrakt, bliver de orienteret om reglerne og procedurerne for sikkerhedsbeskyttelse af EUCI og har anerkendt deres ansvar med hensyn til beskyttelse af sådanne informationer.

KAPITEL 4

BESØG I FORBINDELSE MED KLASSIFICEREDE TILSKUDSAFTALER

Artikel 8

Grundprincipper

1. Hvis den tilskudsgivende myndighed, eksperter, tilskudsmodtagere 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 tilskudsaftale, arrangeres sådanne besøg i samråd med de pågældende NSA'er eller 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 det klassificerede tilskud

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 det klassificerede tilskud.

Artikel 9

Besøgsanmodninger

1. Tilskudsmodtageres eller underkontrahenters besøg på andre tilskudsmodtageres eller underkontrahenters 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 eller 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 den tilskudsgivende myndigheds lokaliteter)

c) den sikkerhedsansvarlige for den facilitet, der sender den besøgende, modtager derpå via sin egen NSA eller DSA svaret fra NSA'en eller 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. Den tilskudsgivende myndigheds tjenestemænds, eksperters eller revisorers besøg på tilskudsmodtageres eller underkontrahenters 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 sikkerheds-myndighed

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 derefter 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 10

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 eller 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 11

Besøg, der arrangeres direkte

1. I forbindelse med specifikke projekter kan de relevante NSA'er eller DSA'er og Kommissionens sikkerhedsmyndighed aftale en procedure, hvorved besøg vedrørende et specifikt tilskud 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 9 og artikel 10, 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 9 og artikel 10, stk. 1.

KAPITEL 5

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

Artikel 12

Grundprincipper

Den tilskudsgivende 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 tilskudsaftale, herunder udstederens samtykke.

Artikel 13

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 tilskudsmodtager og bruges til at håndtere EUCI i forbindelse med opfyldelsen af tilskudsaftalen (tilskudsmodtagerens 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 tilskudsmodtagers CIS, som bruges til at håndtere EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED og eventuelle sammenkoblinger kan uddelegeres til en tilskudsmodtagers sikkerhedsansvarlige, såfremt dette er tilladt i henhold til nationale love og forskrifter. Hvis denne opgave er uddelegeret, er tilskudsmodtageren 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 eller DSA'er og SAA'er har imidlertid stadig ansvaret for at sikkerhedsbeskytte RESTREINT UE/EU RESTRICTED-informationer, som håndteres af tilskudsmodtageren, samt retten til at kontrollere de sikkerhedsforanstaltninger, som tilskudsmodtageren har truffet. Desuden afleverer tilskudsmodtageren en erklæring til den tilskudsgivende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente nationale SAA, som certificerer, at tilskudsmodtagerens CIS og relaterede sammenkoblinger er akkrediteret til håndtering af EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED ([11]).

Artikel 14

Transport med kurertjenester

Transport af EUCI med kurertjenester skal overholde de relevante bestemmelser i Kommissionens afgørelse (EU, Euratom) 2019/1962 ([12]) om gennemførelsesbestemmelser om håndtering af RESTREINT UE/EU RESTRICTED-informationer og Kommissionens afgørelse (EU, Euratom) 2019/1961 ([13]) om gennemførelsesbestemmelser om håndtering af CONFIDENTIEL UE/EU CONFIDENTIAL- og SECRET UE/EU SECRET-informationer.

Artikel 15

Håndbåren transport

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

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

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

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 tilskudsmodtagerens 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.

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

([12]) Kommissionens afgørelse (EU, Euratom) 2019/1962 af 17. oktober 2019 om gennemførelsesbestemmelser om håndtering af RESTREINT UE/EU RESTRICTED-informationer (EUT L 311 af 2.12.2019, s. 21).

([13]) Kommissionens afgørelse (EU, Euratom) 2019/1961 af 17. oktober 2019 om gennemførelsesbestemmelser om håndtering af CONFIDENTIEL UE/EU CONFIDENTIAL- og SECRET UE/EU SECRET-informationer (EUT L 311 af 2.12.2019, s. 1).

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 tilskudsmodtagerens 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 eller 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 eller 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 tilskudsmodtagerens 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 16

Beredskabsplaner og genoprettende foranstaltninger

Den tilskudsgivende myndighed sikrer, at klassificerede tilskudsaftaler indeholder bestemmelser om, at en tilskudsmodtager udarbejder beredskabsplaner til sikkerhedsbeskyttelse af EUCI, der håndteres i forbindelse med opfyldelsen af det klassificerede tilskud, 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. Tilskudsmodtageren meddeler den tilskudsgivende myndighed sin beredskabsplan.

Artikel 17

Ikrafttræden

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

Udfærdiget i Bruxelles, den 10. februar 2021.

På Kommissionens vegne
For formanden
Johannes HAHN
Medlem af Kommissionen

BILAG I

STANDARDOPLYSNINGER I UDBUDDET

(tilpasses det pågældende udbud)

Sikkerhed

Projekter, der indebærer adgang til EU-klassificerede informationer, skal sikkerhedskontrolleres for at autorisere tilskud og kan være omfattet af specifikke regler for sikkerhedsbeskyttelse (som nærmere beskrevet i de særlige sikkerhedsbetingelser (SAL), der er vedlagt som bilag til tilskudsaftalen).

Disse regler (reguleret ved Kommissionens afgørelse (EU, Euratom) 2015/444 ([1]) og/eller nationale regler) fastsætter f.eks., at:

— projekter, som indebærer informationer, der er klassificeret TRÈS SECRET UE/EU TOP SECRET (eller tilsvarende), **IKKE** kan finansieres

— klassificerede informationer skal markeres i overensstemmelse med de gældende sikkerhedsinstruktioner i de særlige sikkerhedsbetingelser

— informationer med klassifikationsgrad CONFIDENTIEL UE/EU CONFIDENTIAL eller højere (og RESTREINT UE/EU RESTRICTED såfremt det kræves i henhold til nationale regler) kan f.eks.:

  — kun udarbejdes og tilgås på lokaliteter, hvor der foretages facilitetssikkerhedsgodkendelse af den kompetente nationale sikkerhedsmyndighed (NSA), i overensstemmelse med de nationale regler

  — kun håndteres i et sikret område, som er akkrediteret af den kompetente NSA

  — kun tilgås og håndteres af personer med gyldig personelsikkerhedsgodkendelse (PSC) og et need to know

— de klassificerede informationer skal, når tilskuddet udløber, enten returneres eller fortsat beskyttes i overensstemmelse med de gældende regler

— projektopgaver, der indebærer EU-klassificerede informationer (EUCI), kan udelukkende udbydes i underentreprise, hvis den tilskudsgivende myndighed har givet skriftligt samtykke dertil og udelukkende til enheder, der er etableret i en medlemsstat eller i et tredjeland, der har indgået en aftale om informationssikkerhed med EU (eller en administrativ ordning med Kommissionen)

— videregivelse af EUCI til tredjeparter kan ske efter forudgående skriftlig tilladelse fra den tilskudsgivende myndighed.

Bemærk, at der kan kræves en facilitetssikkerhedsgodkendelse før indgåelse af tilskudsaftalen afhængigt af aktivitetstypen. Den tilskudsgivende myndighed vurderer, om der er behov for godkendelser i hvert enkelt tilfælde og fastsætter udstedelsesdatoen herfor i forbindelse med forberedelsen af tilskuddet. Det bemærkes, at vi under **ingen omstændigheder** kan indgå en tilskudsaftale, før mindst én af tilskudsmodtagerne i et konsortium har en facilitetssikkerhedsgodkendelse.

Yderligere sikkerhedsanbefalinger kan blive føjet til tilskudsaftalen i form af sikkerhedsprocedurer (*f.eks. oprettelse af gruppe af sikkerhedsrådgivere, begrænsning af detaljeringsniveau, anvendelse af fake scenario, udelukkelse af klassificerede informationer, m.v.*).

Tilskudsmodtagere skal sikre, at deres projekter ikke er underlagt nationale/tredjelandes sikkerhedskrav, der vil kunne påvirke gennemførelsen eller rejse tvivl om indgåelse af tilskudsaftalen (*f.eks. teknologiske begrænsninger, national klassifikation, m.m.*). Den tilskudsgivende myndighed skal straks underrettes om eventuelle sikkerhedsproblemer.

(Yderligere OPTION for FPA'er: Ved partnerskabsrammeaftaler kan det være nødvendigt at sikkerhedskontrollere både ansøgninger om partnerskabsrammeaftaler og ansøgninger om tilskud.)

([1]) Se Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU-klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).

BILAG II

STANDARDKLAUSULER I TILSKUDSAFTALER

(tilpasses den pågældende tilskudsaftale)

13.2 Sikkerhed — Klassificerede informationer

Parterne skal håndtere klassificerede informationer (EU's eller nationale) i overensstemmelse med gældende EU-ret eller national ret for så vidt angår klassificerede informationer (særlig Kommissionens afgørelse (EU, Euratom) 2015/444 ([1]) og gennemførelsesbestemmelserne dertil).

Specifikke regler for sikkerhedsbeskyttelse (hvis det er relevant) findes i bilag 5.

BILAG 5

Sikkerhed – EU-klassificerede informationer

(OPTION for projekter med EU-klassificerede informationer (standard): Hvis EU-klassificerede informationer anvendes eller frembringes i forbindelse med projektet, skal de behandles i overensstemmelse med klassifikationsvejledningen (SCG) og de særlige sikkerhedsbetingelser (SAL) som fastsat i bilag 1 samt afgørelse (EU, Euratom) 2015/444 og gennemførelsesbestemmelserne dertil, indtil de er blevet afklassificeret.

Produkter, der indeholder EU-klassificerede informationer, skal leveres i overensstemmelse med de særlige procedurer, der er aftalt med den tilskudsgivende myndighed.

Projektopgaver, der indebærer EU-klassificerede informationer, kan udelukkende udbydes i underentreprise, hvis den tilskudsgivende myndighed har givet udtrykkeligt skriftligt samtykke dertil og udelukkende til enheder, der er etableret i en medlemsstat eller i et tredjeland, der har indgået en aftale om informationssikkerhed med EU (eller en administrativ ordning med Kommissionen).

EU-klassificerede informationer må ikke videregives til en tredjepart (heriblandt deltagere, der er involveret i gennemførelse af projektet) uden forudgående udtrykkelig skriftlig godkendelse fra den tilskudsgivende myndighed.)

([1]) Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU-klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).

BILAG III

[Bilag IV (til ……)]

SÆRLIGE SIKKERHEDSBETINGELSER (SAL) [1]

[Standardskabelon]

[1] Nærværende standardskabelon for SAL finder anvendelse, når Kommissionen anses for at være udstederen af de klassificerede informationer, som udarbejdes og håndteres i forbindelse med opfyldelsen af tilskudsaftalen. Hvis Kommissionen ikke er udstederen af de klassificerede informationer, som udarbejdes og håndteres i forbindelse med opfyldelsen af tilskudsaftalen, og hvis medlemsstater, der deltager i tilskuddet, har vedtaget særlige sikkerhedsregler, kan andre standardskabeloner for SAL finde anvendelse.

Tillæg A

SIKKERHEDSKRAV

Den tilskudsgivende myndighed skal indarbejde følgende sikkerhedskrav i de særlige sikkerhedsbetingelser (SAL). Nogle af klausulerne gælder muligvis ikke for tilskudsaftalen. 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 tilskud.

ALMINDELIGE BETINGELSER (*N.B.: gælder for alle klassificerede tilskudsaftaler*)

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

2. Tilskudsmodtagere er omfattet af forpligtelserne i Kommissionens afgørelse (EU, Euratom) 2015/444 ([2]) (herefter benævnt »afgørelse 2015/444«) og gennemførelsesbestemmelserne dertil ([3]). Hvis tilskudsmodtageren står over for et problem med hensyn til anvendelse af den gældende retlige ramme i en medlemsstat, skal tilskudsmodtageren henvende sig til Kommissionens sikkerhedsmyndighed og den nationale sikkerhedsmyndighed (NSA) eller den udpegede sikkerhedsmyndighed (DSA).

3. Klassificerede informationer, der frembringes under opfyldelsen af tilskudsaftalen, 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 tilskudsgivende myndighed.

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

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

6. Hvis der kræves en FSC til opfyldelse af en tilskudsaftale, skal tilskudsmodtageren anmode den tilskudsgivende myndighed om at behandle FSC-anmodningen.

7. Tilskudsmodtageren skal undersøge alle sikkerhedsbrister, der vedrører EUCI, og indberette dem til den tilskudsgivende myndighed så hurtigt som praktisk muligt. Tilskudsmodtageren og 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 tilskudsaftalen, 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.

([2]) Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU-klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).

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

8. Når tilskudsaftalen udløber, skal tilskudsmodtageren eller underkontrahenten returnere alle EUCI, som vedkommende er i besiddelse af, til den tilskudsgivende myndighed så hurtigt som muligt. Hvis det er mere praktisk, kan tilskudsmodtageren 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 tilskudsmodtageren 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.

9. Hvis tilskudsmodtageren eller underkontrahenten har autorisation til at beholde EUCI efter tilskudsaftalens ophævelse eller opfyldelse, skal de pågældende EUCI fortsat beskyttes i henhold til afgørelse 2015/444 og gennemførelsesbestemmelserne dertil ([4]).

10. Elektronisk håndtering, behandling og transmission af EUCI skal ske i overensstemmelse 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 tilskudsmodtageren og bruges til at håndtere EUCI i forbindelse med opfyldelsen af tilskudsaftalen (herefter benævnt »tilskudsmodtagerens CIS«), skal akkrediteres ([5]), 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.

11. Tilskudsmodtageren eller underkontrahenten skal have beredskabsplaner til sikkerhedsbeskyttelse af EUCI, der håndteres i forbindelse med opfyldelsen af den klassificerede tilskudsaftale, 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. Tilskudsmodtageren eller underkontrahenten skal orientere den tilskudsgivende myndighed sin beredskabsplan.

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

12. I princippet kræves ingen personelsikkerhedsgodkendelse (PSC) i forbindelse med overholdelsen af tilskudsaftalen ([6]). Informationer eller materiale, der er klassificeret RESTREINT UE/EU RESTRICTED, må imidlertid kun være tilgængeligt for de af tilskudsmodtagerens ansatte, som har behov herfor med henblik på opfyldelsen af tilskudsaftalen (need to know-princippet), som af tilskudsmodtagerens 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.

13. Medmindre den tilskudsgivende myndighed har givet skriftlig godkendelse hertil, må tilskudsmodtageren 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.

14. Tilskudsmodtageren eller underkontrahenten skal bevare klassifikationsmærkningerne på klassificerede informationer, der frembringes af eller viderebringes under opfyldelsen af en tilskudsaftale, og må ikke afklassificere informationer uden skriftligt samtykke fra den tilskudsgivende myndighed.

15. 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, og emballagen må ikke åbnes undervejs.

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

([5]) Den part, der foretager akkrediteringen, skal aflevere en overensstemmelseserklæring til den tilskudsgivende myndighed via Kommissionens sikkerhedsmyndighed og i samarbejde med den relevante nationale sikkerhedsakkrediteringsmyndighed (SAA).

([6]) Hvis tilskudsmodtageren er fra en medlemsstat, der kræver PSC'er og/eller FSC'er for tilskud, der er klassificeret RESTREINT UE/EU RESTRICTED, angiver den tilskudsgivende myndighed disse PSC- og FSC-krav i SAL for de pågældende tilskudsmodtagere.

16. Tilskudsmodtageren 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 tilskudsmodtageren eller underkontrahenten følge programmets eller projektets sikkerhedsinstruktion (PSI) som udstedt af Kommissionen og/eller Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede tilskudsaftaler ([7]).

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

18. Sikkerhedsakkrediteringen af en tilskudsmodtagers CIS, som bruges til at håndtere EUCI med klassifikationsgraden RESTREINT UE/EU RESTRICTED, og eventuelle sammenkoblinger kan uddelegeres til en tilskudsmodtagers 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 tilskudsmodtageren, samt retten til at kontrollere de sikkerhedsforanstaltninger, som tilskudsmodtageren har truffet. Desuden afleverer tilskudsmodtageren en erklæring til den tilskudsgivende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente nationale SAA, som certificerer, at tilskudsmodtagerens 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)

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

BETINGELSER HVORPÅ TILSKUDSMODTAGEREN KAN UDBYDE DELE AF TILSKUDSAFTALEN I UNDERENTREPRISE

20. Tilskudsmodtageren skal indhente tilladelse fra den tilskudsgivende myndighed, inden en del af en klassificeret tilskudsaftale udbydes i underentreprise.

21. 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.

22. Hvis en tilskudsmodtager har tildelt en underkontrakt, finder tilskudsaftalens sikkerhedsbestemmelser tilsvarende anvendelse på underkontrahenten og dennes ansatte. I sådanne tilfælde er det tilskudsmodtagerens ansvar at sikre, at alle underkontrahenter anvender disse bestemmelser på deres egne underentrepriseaftaler. For at sikre passende tilsyn med sikkerheden skal tilskudsmodtagerens og underkontrahentens NSA og/eller DSA underrettes af Kommissionens sikkerhedsmyndighed om tildelingen af relaterede klassificerede underkontrakter med klassifikationsgraden CONFIDENTIEL UE/EU CONFIDENTIAL og SECRET UE/EU SECRET. Tilskudsmodtagerens og underkontrahentens NSA og/eller 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 tilskudsaftaler med klassifikationsgraden RESTREINT UE/EU RESTRICTED, er opført i bilaget til Kommissionens gennemførelsesbestemmelser om industrisikkerhed for så vidt angår klassificerede tilskudsaftaler ([8]).

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

([7]) Den tilskudsgivende myndighed bør indsætte henvisning hertil, så snart gennemførelsesbestemmelserne er vedtaget.
([8]) Den tilskudsgivende myndighed bør indsætte henvisning hertil, så snart gennemførelsesbestemmelserne er vedtaget.

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 tilskudsgivende myndighed indarbejde stk. 24, 25 og 26 og slette stk. 27. 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 tilskudsgivende myndighed slette stk. 25 og 26 og kun indarbejde stk. 27.

24. 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. 25 til 27 nedenfor.

(25. 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 eller DSA.

b) NSA'en/DSA'en for den facilitet, der sender den besøgende, bekræfter den besøgendes PSC, før besøgsanmodningen fremsendes til NSA'en eller 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 eller DSA svaret fra NSA'en eller 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.)

(26. 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 eller DSA.)

(27. 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).)

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

29. 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 fem år eller i overensstemmelse med nationale love og forskrifter, alt efter hvad der er relevant.

VURDERINGSBESØG

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

KLASSIFIKATIONSVEJLEDNING

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

Tillæg B

KLASSIFIKATIONSVEJLEDNING

(den specifikke tekst tilpasses tilskudsaftalens 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/DA, 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-mailadresse. Angiv navn og telefonnummer/faxnummer og e-mail 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 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 (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 (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 ([9]).

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

([9]) 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.

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:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

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 ([10]) gennemføres.>

([10]) 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. hvordan artikel 13 i databeskyttelsesforordningen ([11]) gennemføres.>

([11]) 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. hvordan artikel 13 i databeskyttelsesforordningen ([12]) gennemføres.>

([12]) 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 tilskudsgivende myndighed) vedrørende facilitetssikkerhedsgodkendelsen af en facilitet, der er berørt af en tilbudsaftale eller en underkontrakt.

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

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 eller DSA, der indgiver ansøgningen, i ansøgningens felt nr. 7.

1.4. Oplysningerne i 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 et tilskud eller en underkontrakt i overensstemmelse med en FSC-erklæring, skal den NSA eller DSA, der udsteder facilitetssikkerhedsgodkendelsen, underrettes.

Procedurer og vejledning I anvendelsen af oplysningsskemaet vedrørende facilitetssikkerhedsgodkendelse (FSC-oplysningsskema)

Denne detaljerede vejledning er tiltænkt den NSA eller DSA eller Kommissionen som tilskudsgivende 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 tilskudsgivende 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, udbuds- eller tilskudsnummer. 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, tilskudsmodtageren 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 FACILITETSSIKKERHEDSGODKENDELSES-ERKLÆRING

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 tilskudsmodtager 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 på den sikkerhedsansvarlige

....

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

.....

NSA/DSA/Kommissionen som tilskudsgivende 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. hvordan artikel 13 i databeskyttelsesforordningen ([13]) gennemføres.>

([13]) 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 tilskudsmodtagerens CIS

Generelt

1. Tilskudsmodtageren 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 tilskudsgivende myndighed eller, hvis det relevant, den nationale sikkerhedsmyndighed (NSA) eller den udpegede sikkerhedsmyndighed (DSA).

2. Det er tilskudsmodtagerens 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. Tilskudsmodtageren 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 tilskudsmodtagerens ansatte, må ikke anvendes til lagring eller behandling af RESTREINT UE/EU RESTRICTED-informationer.

7. Akkreditering af tilskudsmodtagerens CIS, som håndterer informationer, der er klassificeret RESTREINT UE/EU RESTRICTED, skal godkendes af sikkerhedsakkrediteringsmyndigheden (SAA) i den relevante medlemsstat eller uddelegeres til tilskudsmodtagerens 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 tilskudsaftalen, 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 tilskudsgivende myndighed eller den relevante NSA/DSA/SAA skal tilskudsmodtageren dokumentere overholdelse af sikkerhedsklausulen for tilskudsaftalen. Hvis der også anmodes om en revision og kontrol af tilskudsmodtagerens procedurer og faciliteter med henblik på at sikre overholdelse af kravene, skal tilskudsmodtageren give repræsentanter for den tilskudsgivende myndighed, NSA'en, DSA'en og/eller 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 tilskudsmodtagers 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 ændres 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 bruger-id. 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) bruger-id

    c) dato og tidspunkt

    d) udstyrets id-nummer.

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. Tilskudsmodtageren 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 tilskudsgivende 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 tilskudsmodtagers 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 tilskudsmodtageren eller underkontrahenten. Hvis dette er tilfældet, skal tilskudsmodtageren foretage en risikovurdering med henblik på at udpege yderligere sikkerhedskrav, der skal opfyldes i forbindelse med sikkerhedsakkrediteringsprocessen. Tilskudsmodtageren skal aflevere en erklæring til den tilskudsgivende myndighed og, såfremt det kræves i henhold til nationale love og forskrifter, den kompetente SAA, som certificerer, at tilskudsmodtagerens 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 tilskudsgivende 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. Tilskudsmodtagerens sikkerhedsansvarlige skal udføre konfigurationskontrol på såvel hardware som software for at sikre, at der ikke anvendes uautoriseret hardware eller software.

30. Ændringer i tilskudsmodtagerens 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. Tilskudsmodtageren 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 rensning 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 tilskudsgivende myndighed eller, hvis det er relevant, NSA, DSA eller 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 tilskudsmodtagere eller underkontrahenter, som omfatter adgang til RESTREINT UE/EU RESTRICTED-informationer, og NSA'er/DSA'er, der kræver underretning om klassificerede tilskudsaftaler med klassifikationsgraden RESTREINT UE/EU RESTRICTED ([1])

Medlemsstat	FSC		Underretning om tilskudsaftaler eller underkontrakter, der omfatter adgang til R-UE/EU-R-informationer til NSA'en og/eller 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**
Litauen	**X**		**X**			**X**
Luxembourg	**X**		**X**		**X**	
Ungarn		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nederlandene	**X** (kun tilskudsaftaler og underkontrakter, der vedrører forsvar)		**X** (kun tilskudsaftaler og underkontrakter, der vedrører forsvar)			**X**
Østrig		**X**		**X**		**X**
Polen		**X**		**X**		**X**

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

Portugal		**X**		**X**		**X**
Rumænien		**X**		**X**		**X**
Slovenien	**X**		**X**			**X**
Slovakiet	**X**		**X**			**X**
Finland		**X**		**X**		**X**
Sverige		**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

E-mail: 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
   E-mail: 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
   E-mail: office@iksbg.org

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

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tlf. +359 29824971
   Fax +359 29461339
   E-mail: 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

   E-mail: 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

E-mail: 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 København Ø

   Tlf. +45 33325566

   Fax +45 33931320

TYSKLAND

1. Spørgsmål vedrørende industrisikkerhedspolitik, FSC og transportplaner (med undtagelse af krypto-/fortrolige forretningsoplysninger):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Tlf. +49 228996154028

   Fax +49 228996152676

   E-mail: dsagermany-rs3@bmwi.bund.de (office email address)

2. Standardbesøgsanmodninger fra/til tyske virksomheder:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division — RS2
Villemombler Str. 76
53123 Bonn

Tlf. +49 228996152401

Fax +49 228996152603

E-mail: rs2-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

E-mail: NDAEU@bsi.bund.de

ESTLAND

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallin

Tlf. +372 6939211

Fax +372 6935001

E-mail: 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

E-mail: 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

E-mail: daa.industrial@hndgs.mil.gr

SPANIEN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid

Tlf. +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

E-mail: nsa-sp@areatec.com

Klassificerede programmer: programas.ons@areatec.com

Personelsikkerhedsgodkendelser: hps.ons@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

E-mail: 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

E-mail: 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

E-mail: 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

E-mail: 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

E-mail: 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

E-mail: ndi@sab.gov.lv, 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
Pilaitės pr. 19
LT-06264 Vilnius

Tlf. +370 70666128

E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg

Tlf. +352 24782210

E-mail: 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

E-mail: 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

E-mail: 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

   E-mail: 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

   E-mail: indussec@mindef.nl

ØSTRIG

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tlf. +43 153115202594

   E-mail: isk@bka.gv.at

2. DSA in the military sphere:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   E-mail: 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

E-mail: 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

E-mail: 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

E-mail: 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

E-mail: 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

E-mail: podatelna@nbu.gov.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

E-mail: 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
   E-mail: ud-nsa@gov.se

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