KOMMISSIONENS BESLUT (EU, Euratom) 2021/259

av den 10 februari 2021

om tillämpningsföreskrifter för industrisäkerhet avseende säkerhetsskyddsklassificerade bidrag

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

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

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

med beaktande av Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (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 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012 ([1]),

med beaktande av kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen ([2]),

med beaktande av kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter ([3]),

med beaktande av kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem ([4]),

efter att ha hört kommissionens grupp av säkerhetsexperter i enlighet med artikel 41.5 i beslut (EU, Euratom) 2015/444, och

av följande skäl:

(1) Artiklarna 41, 42, 47 och 48 i beslut (EU, Euratom) 2015/444 fastställer att närmare bestämmelser för att komplettera eller understödja kapitel 6 i det beslutet ska antas i tillämpningsföreskrifter om industrisäkerhet i sådana frågor som tilldelning av säkerhetsskyddsklassificerade bidragsavtal, säkerhetsgodkännande av verksamhetsställe, personalsäkerhetsgodkännande, besök samt överföring och befordran av säkerhetsskyddsklassificerade EU-uppgifter.

(2) Enligt beslut (EU, Euratom) 2015/444 föreskrivs att säkerhetsskyddsklassificerade bidragsavtal ska fullgöras i nära samarbete med den nationella säkerhetsmyndigheten, den utsedda säkerhetsmyndigheten eller någon annan behörig myndighet i den berörda medlemsstaten. Medlemsstaterna har enats om att se till att alla de enheter inom deras jurisdiktion som eventuellt kan erhålla eller generera säkerhetsskyddsklassificerade uppgifter som härrör från kommissionen har genomgått lämplig säkerhetsprövning och kan ge ett ändamålsenligt skydd, på en lämplig säkerhetsnivå som är likvärdig med den som ges enligt säkerhetsbestämmelserna inom Europeiska unionens råd för säkerhetsskyddsklassificerade EU-uppgifter med motsvarande säkerhetsklassning i enlighet med avtalet mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse (2011/C 202/05) ([5]).

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

(3) Rådet, kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik har enats om att säkerställa maximal konsekvens i tillämpningen av säkerhetsbestämmelserna avseende sitt skydd av säkerhetsskyddsklassificerade EU-uppgifter, med samtidig hänsyn till sina specifika institutionella och organisatoriska behov i enlighet med de förklaringar som fogades till protokollet från det möte där rådets beslut 2013/488/EU ([6]) om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter antogs.

(4) Kommissionens tillämpningsföreskrifter för industrisäkerhet avseende säkerhetsskyddsklassificerade bidrag bör därför också säkerställa maximal konsekvens och beakta de riktlinjer för industrisäkerhet som antogs av rådets säkerhetskommitté den 13 december 2016.

(5) Den 4 maj 2016 antog kommissionen ett beslut ([7]) om delegering av befogenheter till den ledamot av kommissionen som ansvarar för säkerhetsfrågor för att, på kommissionens vägnar och på dess ansvar, anta de tillämpningsföreskrifter som avses i artikel 60 i beslut (EU, Euratom) 2015/444.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. Detta beslut fastställer tillämpningsföreskrifter för industrisäkerhet avseende säkerhetsskyddsklassificerade bidrag i den mening som avses i beslut (EU, Euratom) 2015/444, särskilt kapitel 6 i det beslutet.

2. Detta beslut fastställer särskilda krav för att säkerställa att säkerhetsskyddsklassificerade EU-uppgifter skyddas i samband med offentliggörande av ansökningsomgångar och vid beviljande av bidrag och genomförande av säkerhetsskyddsklassificerade bidragsavtal som ingås av Europeiska kommissionen.

3. Detta beslut avser bidrag som innefattar uppgifter som säkerhetsklassats på följande nivåer:

a) RESTREINT UE/EU RESTRICTED.

b) CONFIDENTIEL UE/EU CONFIDENTIAL.

c) SECRET UE/EU SECRET.

4. Detta beslut påverkar inte tillämpningen av specifika regler som fastställs i andra rättsakter, exempelvis de som rör det europeiska försvarsindustriella utvecklingsprogrammet.

Artikel 2

Kommissionens ansvarsområden

1. Som ett led i ansvaret för utanordnaren vid den bidragsbeviljande myndigheten såsom avses i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 ska denne säkerställa att säkerhetsskyddsklassificerade bidrag efterlever beslut (EU, Euratom) 2015/444 och dess genomförandebestämmelser.

([6]) Rådets beslut 2013/488/EU av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 274, 15.10.2013, s. 1).

([7]) Kommissionens beslut av den 4 maj 2016 om delegering av befogenheter som avser säkerhet [C(2016) 2797 final].

2. Därför ska den berörda utanordnaren i alla stadier inhämta rådgivning från kommissionens säkerhetsmyndighet i frågor som avser säkerhetsinslag i säkerhetsskyddsklassificerade bidragsavtal, program eller projekt och ska informera den lokalt säkerhetsansvariga om de säkerhetsskyddsklassificerade bidragsavtal som undertecknats. Beslut om vilken klassificeringsnivå som ska tilldelas ska fattas av den bidragsbeviljande myndigheten med vederbörlig hänsyn till handboken om säkerhetsklassificering.

3. Om säkerhetsanvisningarna för programmet eller projektet som avses i artikel 5.3 tillämpas ska den bidragsbeviljande myndigheten och kommissionens säkerhetsmyndighet fullgöra de skyldigheter som anvisas dem i dessa anvisningar.

4. Vid genomförandet av kraven i dessa tillämpningsföreskrifter ska kommissionens säkerhetsmyndighet samarbeta nära tillsammans med de berörda medlemsstaternas nationella säkerhetsmyndigheter och utsedda säkerhetsmyndigheter, i synnerhet när det gäller säkerhetsgodkännande av verksamhetsställen och personalsäkerhetsgodkännanden, besöksrutiner och transporter.

5. Om bidrag hanteras av EU:s genomförandeorgan eller andra finansieringsorgan och de specifika bestämmelser som fastställs i andra rättsakter som anges i artikel 1.4 inte är tillämpliga gäller följande:

a) Den delegerande kommissionsavdelningen ska utöva de rättigheter som tillkommer upphovsmannen till säkerhetsskyddsklassificerade EU-uppgifter som genereras inom ramen för bidragen om så föreskrivs i delegeringsarrangemanget.

b) Den delegerande kommissionsavdelningen ska ansvara för beslutet om säkerhetsklassificering.

c) Begäranden om information om säkerhetsgodkännande samt anmälningar till de nationella säkerhetsmyndigheterna och/eller utsedda säkerhetsmyndigheterna ska skickas via kommissionens säkerhetsmyndighet.

KAPITEL 2

HANTERING AV ANSÖKNINGSOMGÅNGAR FÖR SÄKERHETSSKYDDSKLASSIFICERADE BIDRAG

Artikel 3

Grundprinciper

1. Säkerhetsskyddsklassificerade delar av bidraget får endast genomföras av bidragsmottagare som är registrerade i en medlemsstat eller som är registrerade i ett sådant tredjeland eller är inrättade genom en sådan internationell organisation som slutit informationssäkerhetsavtal med EU eller ingått en administrativ överenskommelse med kommissionen ([8]).

2. Innan ansökningsomgångar för ett säkerhetsskyddsklassificerat bidrag inleds ska den bidragsbeviljande myndigheten fastställa säkerhetsklassificeringen för alla uppgifter som kan komma att tillhandahållas de sökande. Den bidragsbeviljande myndigheten ska även fastställa den högsta säkerhetsklassificeringsnivån för alla uppgifter som kommer att användas eller genereras vid fullgörandet av bidragsavtalet, programmet eller projektet, eller åtminstone den förväntade omfattningen och typen av uppgifter som ska framställas eller hanteras samt behovet av ett säkerhetsklassat kommunikations- och informationssystem.

3. Den bidragsbeviljande myndigheten ska säkerställa att det under ansökningsomgångar för säkerhetsskyddsklassificerade bidrag ges upplysningar om de särskilda säkerhetskrav som ställs avseende säkerhetsskyddsklassificerade uppgifter. Ansökningsdokumentationen ska innefatta förtydliganden om tidsfristen för bidragsmottagare att erhålla säkerhetsgodkännande av verksamhetsställe när så krävs. Bilagorna I och II innehåller ett förslag på mall för information avseende ansökningsvillkoren.

([8]) Förteckningen över EU:s avtal och Europeiska kommissionens administrativa överenskommelser om utbyte av säkerhetsskyddsklassificerade EU-uppgifter med tredjeland och internationella organisationer finns på kommissionens webbplats.

4. Den bidragsbeviljande myndigheten ska säkerställa att uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET yppas för de sökande först när de undertecknat ett sekretessavtal som ålägger dem att hantera och skydda säkerhetsskyddsklassificerade EU-uppgifter i enlighet med beslut (EU, Euratom) 2015/444, dess genomförandebestämmelser och tillämpliga nationella föreskrifter.

5. När uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED tillhandahålls sökande ska de minimikrav som avses i artikel 5.7 i detta beslut tas med i ansökningsdokumentationen eller i det sekretessavtal som ingås i förslagsfasen.

6. Alla sökande och bidragsmottagare som kommer att hantera eller lagra uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i sina lokaler, antingen under förslagsfasen eller under fullgörandet av själva säkerhetsskyddsklassificerade bidragsavtalet, måste inneha ett säkerhetsgodkännande av verksamhetsställe på lämplig nivå, förutom i de fall som nämns i punkt 9. Följande tre scenarier kan uppstå under förslagsfasen för säkerhetsskyddsklassificerade bidrag och som rör säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET:

a) Ingen tillgång till säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i förslagsfasen:

   Om ansökan avser ett bidrag som kommer att omfatta säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET men som inte kräver att den sökande ska hantera uppgifterna i förslagsfasen ska sökande utan säkerhetsgodkännande av verksamhetsställe på lämplig nivå inte uteslutas från ansökningsförfarandet därför att de saknar sådant säkerhetsgodkännande.

b) Tillgång till säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i den bidragsbeviljande myndighetens lokaler i förslagsfasen:

   Tillgång ska beviljas sådan personal från den sökande som innehar personalsäkerhetsgodkännande på lämplig nivå och som har behovsenlig behörighet.

c) Hantering eller lagring av säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i den sökandes lokaler i förslagsfasen:

   Om ansökan kräver att sökande hanterar eller lagrar säkerhetsskyddsklassificerade EU-uppgifter i sina lokaler måste den sökande inneha ett säkerhetsgodkännande av verksamhetsställe på lämplig nivå. I sådana fall ska den bidragsbeviljande myndigheten via kommissionens säkerhetsmyndighet inhämta försäkran från nationell säkerhetsmyndighet eller utsedd säkerhetsmyndighet om att den sökande beviljats det säkerhetsgodkännande av verksamhetsställe som krävs innan den sökande tillhandahålls material som rör säkerhetsskyddsklassificerade EU-uppgifter. Tillgång ska beviljas sådan personal från den sökande som innehar personalsäkerhetsgodkännande på lämplig nivå och som har behovsenlig behörighet.

7. I princip ska säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande inte krävas för tillgång till uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED, vare sig i förslagsfasen eller under fullgörandet av bidragsavtalet. Medlemsstater som kräver säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande för bidragsavtal eller underentreprenörsavtal som rör uppgifter som säkerhetsklassats på nivå RESTREINT UE/EU RESTRICTED enligt den statens nationella lagar och andra föreskrifter, i enlighet med förteckningen i bilaga IV, får i de nationella kraven inte ställa ytterligare krav på andra medlemsstater eller utesluta sökande, bidragsmottagare eller underentreprenörer med säte i sådana medlemsstater som inte kräver säkerhetsgodkännande av verksamhetsställe eller personalsäkerhetsgodkännande för tillgång till uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED eller utestänga dem från sådana bidragsavtal eller underentreprenörsavtal eller från upphandlingen. Sådana bidragsavtal ska fullgöras i medlemsstaterna i enlighet med deras nationella lagar och andra föreskrifter.

8. Om säkerhetsgodkännande av verksamhetsställe krävs i samband med hanteringen av en ansökan och för fullgörande av ett säkerhetsskyddsklassificerat bidragsavtal ska den bidragsbeviljande myndigheten, via kommissionens säkerhetsmyndighet, lämna in en begäran till bidragsmottagarens nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet med hjälp av ett informationsblad för säkerhetsgodkännande av verksamhetsställe eller annat fastställt likvärdigt elektroniskt format. I tillägg D i bilaga III finns ett exempel på informationsblad för säkerhetsgodkännande av verksamhetsställe ([9]). Svar på informationsblad för säkerhetsgodkännande av verksamhetsställe ska så långt som möjligt lämnas inom tio arbetsdagar från den dag begäran gjordes.

9. Om medlemsstaternas förvaltningsinrättningar eller inrättningar under tillsyn av regeringen deltar i säkerhetsskyddsklassificerade bidrag som kräver säkerhetsgodkännande av verksamhetsställe och där sådana säkerhetsgodkännanden inte utfärdas för sådana inrättningar enligt nationell lagstiftning ska den bidragsbeviljande myndigheten, via kommissionens säkerhetsmyndighet, verifiera med den berörda nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten om dessa förvaltningsinrättningar har kapacitet att hantera säkerhetsskyddsklassificerade EU-uppgifter på den erfordrade nivån.

([9]) Andra formulär kan ha en annan utformning än förlagan i dessa tillämpningsföreskrifter.

10. Om personalsäkerhetsgodkännande krävs för fullgörande av ett säkerhetsskyddsklassificerat bidragsavtal och om ett säkerhetsgodkännande av verksamhetsställe enligt nationella regler krävs innan ett personalsäkerhetsgodkännande beviljas ska den bidragsbeviljande myndigheten, via kommissionens säkerhetsmyndighet, med hjälp av ett informationsblad för säkerhetsgodkännande av verksamhetsställe kontrollera med bidragsmottagarens nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet att bidragsmottagaren innehar säkerhetsgodkännande av verksamhetsställe eller att förfarandet för erhållande av säkerhetsgodkännande av verksamhetsställe pågår. I detta fall ska kommissionen inte utfärda en begäran om personalsäkerhetsgodkännande med hjälp av informationsblad för personalsäkerhetsgodkännande.

Artikel 4

Underentreprenad inom ramen för säkerhetsskyddsklassificerade bidrag

1. Villkoren på vilka bidragsmottagare får lägga ut uppgifter som inbegriper säkerhetsskyddsklassificerade EU-uppgifter på underentreprenad ska anges i ansökningsdokumentationen och i bidragsavtalet. Dessa villkor ska innefatta ett krav på att alla informationsblad för säkerhetsgodkännande av verksamhetsställe ska lämnas in genom kommissionens säkerhetsmyndighet. Underentreprenad förutsätter skriftligt förhandsmedgivande från den bidragsbeviljande myndigheten. I tillämpliga fall ska underentreprenaden uppfylla den rättsliga grunden för inrättande av programmet.

2. Säkerhetsskyddsklassificerade delar av bidraget får endast läggas ut på underentreprenad till personer som är registrerade i en medlemsstat eller som är registrerade i ett sådant tredjeland eller är inrättade genom en sådan internationell organisation som slutit informationssäkerhetsavtal med EU eller ingått en administrativ överenskommelse med kommissionen ([10]).

KAPITEL 3

HANTERING AV SÄKERHETSSKYDDSKLASSIFICERADE BIDRAG

Artikel 5

Grundprinciper

1. Vid tilldelning av ett säkerhetsskyddsklassificerat bidrag ska den bidragsbeviljande myndigheten tillsammans med kommissionens säkerhetsmyndighet säkerställa att man i en del av bidragsavtalet preciserar bidragsmottagarens skyldigheter i fråga om säkerhetsskyddsklassificerade EU-uppgifter som används eller som genereras vid fullgörandet av bidragsavtalet. Säkerhetskrav som är specifika för bidraget ska utformas som en säkerhetsskyddsöverenskommelse. Ett förslag på mall till säkerhetsskyddsöverenskommelse finns i bilaga III.

2. Innan ett säkerhetsskyddsklassificerat bidrag undertecknas ska den bidragsbeviljande myndigheten godkänna en handbok om säkerhetsklassificering för de uppgifter som ska utföras och de upplysningar som genereras vid genomförandet av bidraget, eller i förekommande fall på program- eller projektnivå. Handboken om säkerhetsklassificering ska utgöra en del av säkerhetsskyddsöverenskommelsen.

3. Säkerhetskrav som är specifika för vissa program eller projekt ska utformas som säkerhetsanvisningar för program eller projekt. Säkerhetsanvisningar för program eller projekt kan utarbetas med hjälp av bestämmelserna i mallen till säkerhetsskyddsöverenskommelse i bilaga III. Säkerhetsanvisningar för program eller projekt ska tas fram av den kommissionsavdelning som förvaltar programmet eller projektet i nära samarbete med kommissionens säkerhetsmyndighet och ska lämnas in till kommissionens grupp av säkerhetsexperter för rådgivning. Om ett bidragsavtal ingår i ett program eller projekt med egna säkerhetsanvisningar ska säkerhetsskyddsöverenskommelsen för bidragsavtalet i fråga förenklas och hänvisa till bestämmelserna i det övergripande programmets eller projektets säkerhetsanvisningar.

4. Förutom i fall som anges i artikel 3.9 ska det säkerhetsskyddsklassificerade bidragsavtalet inte undertecknas förrän den sökandes nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet har bekräftat den sökandes säkerhetsgodkännande av verksamhetsställe eller, om det säkerhetsskyddsklassificerade bidragsavtalet tilldelas ett konsortium, förrän den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten för minst en sökande i konsortiet, eller fler om nödvändigt, har bekräftat denne sökandes säkerhetsgodkännande av verksamhetsställe.

5. I princip ska den bidragsbeviljande myndigheten, om inte annat anges i andra relevanta bestämmelser, anses som upphovsman till säkerhetsskyddsklassificerade uppgifter som genereras i samband med fullgörandet av bidragsavtalet.

([10]) Förteckningen över EU:s avtal och Europeiska kommissionens administrativa överenskommelser om utbyte av säkerhetsskyddsklassificerade EU-uppgifter med tredjeland och internationella organisationer finns på kommissionens webbplats.

6. Den bidragsbeviljande myndigheten ska via kommissionens säkerhetsmyndighet underrätta alla bidragsmottagares och underentreprenörers nationella säkerhetsmyndigheter och/eller utsedda säkerhetsmyndigheter varje gång säkerhetsskyddsklassificerade bidragsavtal eller underentreprenörsavtal som kräver säkerhetsavtal undertecknas, förlängs eller sägs upp i förtid. En förteckning över kraven i olika länder finns i bilaga IV.

7. Bidragsavtal som berör uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED ska innehålla en säkerhetsklausul som gör bestämmelserna i tillägg E i bilaga III bindande för bidragsmottagarna. Bidragsavtalen ska innehålla en säkerhetsskyddsöverenskommelse som fastställer minimikrav för hanteringen av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED, däribland krav på informationssäkring och särskilda krav för bidragsmottagarna avseende säkerhetsackreditering av det ikt-system de använder för hantering av uppgifter på nivån RESTREINT UE/EU RESTRICTED.

8. När detta krävs enligt medlemsstaternas nationella lagar och andra föreskrifter ska nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter säkerställa att bidragsmottagare eller underentreprenörer inom deras jurisdiktion uppfyller de tillämpliga säkerhetsbestämmelserna för skydd av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED och ska göra kontrollbesök på bidragsmottagarnas eller underentreprenörernas verksamhetsställen belägna på det egna territoriet. Om den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten inte är underställd något sådant krav ska den bidragsbeviljande myndigheten säkerställa att bidragsmottagaren fullgör säkerhetsbestämmelserna i tillägg E i bilaga III.

Artikel 6

Tillgång till säkerhetsskyddsklassificerade EU-uppgifter för bidragsmottagares och underentreprenörers personal

1. Den bidragsbeviljande myndigheten ska säkerställa att säkerhetsskyddsklassificerade bidragsavtal innehåller bestämmelser om att personal hos bidragsmottagare eller underentreprenörer som behöver få tillgång till säkerhetsskyddsklassificerade EU-uppgifter för att kunna fullgöra det säkerhetsskyddsklassificerade bidragsavtalet eller underentreprenaden beviljas tillgång endast i följande fall:

a) Det har fastställts att vederbörande har behovsenlig behörighet.

b) För uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska vederbörande ha genomgått säkerhetsprövning på lämplig nivå genom sina respektive nationella säkerhetsmyndigheter, utsedda säkerhetsmyndigheter eller andra behöriga säkerhetsmyndigheter.

c) Vederbörande har informerats om de säkerhetsbestämmelser som gäller för säkerhetsskyddsklassificerade EU-uppgifter och har bekräftat sitt ansvar för skyddet av dessa uppgifter.

2. I tillämpliga fall ska tillgången till säkerhetsskyddsklassificerade EU-uppgifter även vara i linje med den rättsliga grunden för inrättande av programmet och ta hänsyn till eventuella uppgifter som anges i handboken om säkerhetsklassificering.

3. Om en bidragsmottagare eller underentreprenör vill anställa en person som är medborgare i tredjeland på en tjänst som kräver tillgång till säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET åligger det bidragsmottagaren eller underentreprenören att begära säkerhetsprövning för personen i enlighet med nationella lagar och andra föreskrifter som är tillämpliga på den ort där tillgången till säkerhetsskyddsklassificerade EU-uppgifter ska medges.

Artikel 7

Tillgång till säkerhetsskyddsklassificerade EU-uppgifter för experter i samband med kontroller, översyner och revisioner

1. Om externa personer (experter) deltar i kontroller, översyner eller revisioner som genomförs av den bidragsbeviljande myndigheten eller inom ramen för resultatöversyner av bidragsmottagare som kräver tillgång till uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska de tillhandahållas ett avtal endast om de har genomgått säkerhetsprövning på lämplig nivå genom sina respektive nationella säkerhetsmyndigheter, utsedda säkerhetsmyndigheter eller andra behöriga säkerhetsmyndigheter. Den bidragsbeviljande myndigheten ska, genom kommissionens säkerhetsmyndighet, kontrollera och, vid behov, be den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten att inleda säkerhetsprövningen för experter minst sex månader innan respektive avtal inleds.

2. Innan de undertecknar sina avtal ska experterna informeras om de säkerhetsbestämmelser som gäller för säkerhetsskyddsklassificerade EU-uppgifter och ha bekräftat sitt ansvar för skyddet av dessa uppgifter.

KAPITEL 4

BESÖK MED ANKNYTNING TILL SÄKERHETSSKYDDSKLASSIFICERADE BIDRAGSAVTAL

Artikel 8

Grundprinciper

1. När den bidragsbeviljande myndigheten, experter, bidragsmottagare eller underentreprenörer behöver få tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET i varandras lokaler inom ramen för genomförandet av ett säkerhetsskyddsklassificerat bidragsavtal, ska besök anordnas tillsammans med de berörda nationella säkerhetsmyndigheterna eller utsedda säkerhetsmyndigheterna eller andra behöriga säkerhetsmyndigheter.

2. Följande krav ska ställas på de besök som avses i punkt 1:

a) Besöket ska ha ett officiellt syfte med anknytning till det säkerhetsskyddsklassificerade bidraget.

b) Alla besökare ska inneha personalsäkerhetsgodkännande på lämplig nivå och ha behovsenlig behörighet för att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter som används eller genereras vid fullgörandet av det säkerhetsskyddsklassificerade bidraget.

Artikel 9

Begäran om besök

1. Bidragsmottagares eller underentreprenörers besök på andra bidragsmottagares eller underentreprenörers verksamhetsställen eller i den bidragsbeviljande myndighetens lokaler som medför tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska anordnas med hjälp av följande förfarande:

a) Den säkerhetsansvariga på det verksamhetsställe som sänder besökaren ska fylla i alla relevanta delar av formuläret för begäran om besök och lämna begäran till verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet. En mall för formulär för begäran om besök finns i tillägg C i bilaga III.

b) Det sändande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet ska bekräfta besökarens personalsäkerhetsgodkännande innan begäran om besök lämnas till det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet (eller kommissionens säkerhetsmyndighet om besöket sker i den bidragsbeviljande myndighetens lokaler).

c) Den säkerhetsansvariga vid det sändande verksamhetsstället ska därefter från sin nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet inhämta det svar som lämnats av det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet (eller av kommissionens säkerhetsmyndighet) varigenom begäran om besök antingen beviljas eller avslås.

d) En begäran om besök anses godkänd om inga invändningar görs fram till fem dagar innan besöket.

2. Besök av den bidragsbeviljande myndighetens tjänstemän eller experter eller revisorer på bidragsmottagares eller underentreprenörers verksamhetsställen som medför tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska anordnas med hjälp av följande förfarande:

a) Besökaren ska fylla i alla relevanta delar av formuläret för begäran om besök och lämna det till kommissionens säkerhetsmyndighet.

b) Kommissionens säkerhetsmyndighet ska bekräfta besökarens personalsäkerhetsgodkännande innan begäran om besök lämnas till det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet.

c) Kommissionens säkerhetsmyndighet ska inhämta det svar som lämnats av det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet varigenom begäran om besök antingen beviljas eller avslås.

d) En begäran om besök anses godkänd om inga invändningar görs fram till fem dagar innan besöket.

3. Begäran om besök kan avse antingen ett besök eller återkommande besök. Vid återkommande besök kan begäran om besök gälla i högst ett år från begärt startdatum.

4. Begäran om besök får inte ha en längre giltighetstid än besökarens personalsäkerhetsgodkännande.

5. Normalt ska begäran om besök lämnas till det mottagande verksamhetsställets behöriga säkerhetsmyndighet minst 15 arbetsdagar innan besöket.

Artikel 10

Besöksrutiner

1. Innan besökare får tillgång till säkerhetsskyddsklassificerade EU-uppgifter ska det mottagande verksamhetsställets säkerhetsbyrå se till att besöket följer alla säkerhetsrutiner och säkerhetsbestämmelser som fastställts av dess nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet.

2. Besökarna ska styrka sin identitet när de anländer till det mottagande verksamhetsstället genom att uppvisa giltig ID-handling eller pass. Identitetsuppgifterna måste motsvara de uppgifter som lämnats på formuläret för begäran om besök.

3. Det mottagande verksamhetsstället ska säkerställa att alla besökare registreras tillsammans med uppgifter om deras namn, den organisation de företräder, sista giltighetsdag för deras personalsäkerhetsgodkännande, besöksdatum och namnet på de besökta personerna. Registren ska sparas i minst fem år, eller längre om detta krävs enligt nationella lagar och andra föreskrifter i det land där det mottagande verksamhetsstället är beläget.

Artikel 11

Besök som anordnas direkt

1. Inom ramen för vissa projekt kan berörda nationella säkerhetsmyndigheter, utsedda säkerhetsmyndigheter eller kommissionens säkerhetsmyndighet enas om ett förfarande som tillåter att besök avseende ett visst säkerhetsskyddsklassificerat bidrag som kräver säkerhetsavtal anordnas gemensamt av den besökandes säkerhetsansvariga och den säkerhetsansvariga vid det verksamhetsställe som ska besökas. En mall för det formulär som kan användas i detta syfte finns i bilaga III tillägg C. Sådana undantagsförfaranden ska beskrivas i säkerhetsanvisningarna för program eller projekt eller i andra särskilda överenskommelser. I dessa fall ska förfarandena i artikel 9 och artikel 10.1 inte tillämpas.

2. Besök som medför tillgång till uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED ska anordnas gemensamt av det besökande och det besökta verksamhetsstället utan att förfarandet i artikel 9 och artikel 10.1 behöver följas.

KAPITEL 5

ÖVERFÖRING OCH BEFORDRAN AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER VID FULLGÖRANDET AV SÄKERHETSSKYDDSKLASSIFICERADE BIDRAGSAVTAL

Artikel 12

Grundprinciper

Den bidragsbeviljande myndigheten ska säkerställa att alla beslut om överföring och befordran av säkerhetsskyddsklassificerade EU-uppgifter följer beslut (EU, Euratom) 2015/444 och dess tillämpningsföreskrifter samt villkoren i det säkerhetsskyddsklassificerade bidragsavtalet, däribland kravet på upphovsmannens medgivande.

Artikel 13

Elektronisk hantering

1. Elektronisk hantering och överföring av säkerhetsskyddsklassificerade EU-uppgifter ska ske i enlighet med kapitel 5 och 6 i beslut (EU, Euratom) 2015/444 och dess tillämpningsföreskrifter.

De kommunikations- och informationssystem som ägs av en bidragsmottagare och som används för att hantera säkerhetsskyddsklassificerade EU-uppgifter vid fullgörandet av bidragsavtalet (nedan kallat *bidragsmottagarens kommunikations- och informationssystem*) ska vara ackrediterat av den ansvariga ackrediteringsmyndigheten för säkerhet. All elektronisk överföring av säkerhetsskyddsklassificerade EU-uppgifter ska skyddas med hjälp av kryptoprodukter som är godkända enligt artikel 36.4 i beslut (EU, Euratom) 2015/444. Tempestsäkerhetsåtgärder ska genomföras i enlighet med artikel 36.6 i det beslutet.

2. Säkerhetsackreditering av bidragsmottagarens kommunikations- och informationssystem för hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED och all sammankoppling av sådana system får delegeras till bidragsmottagarens säkerhetsansvariga om detta är tillåtet enligt nationella lagar och andra föreskrifter. Om uppgiften delegeras ska bidragsmottagaren vara ansvarig för tillämpningen av minimisäkerhetskraven enligt säkerhetsskyddsöverenskommelsen vid hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED i sitt kommunikations- och informationssystem. De berörda nationella säkerhetsmyndigheterna, utsedda säkerhetsmyndigheterna och ackrediteringsmyndigheterna för säkerhet ska dock behålla ansvaret för att skydda uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED som hanteras av bidragsmottagaren och ska ha rätt att inspektera bidragsmottagarens säkerhetsåtgärder. Bidragsmottagaren ska därutöver förse den bidragsbeviljande myndigheten, och där så krävs enligt nationella lagar och andra föreskrifter även den behöriga nationella ackrediteringsmyndigheten för säkerhet, med ett överensstämmelseintyg som styrker att bidragsmottagarens kommunikations- och informationssystem och därmed sammankopplade system har ackrediterats för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED ([11]).

Artikel 14

Transport med kommersiella kurirtjänster

När säkerhetsskyddsklassificerade EU-uppgifter transporteras med kommersiella kurirtjänster ska detta följa relevanta bestämmelser i kommissionens beslut (EU, Euratom) 2019/1962 ([12]) om genomförandebestämmelser för hantering av EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED och kommissionens beslut (EU, Euratom) 2019/1961 ([13]) om genomförandebestämmelser för hantering av EU-uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET.

Artikel 15

Personligt överlämnande

1. Personligt överlämnande av säkerhetsskyddsklassificerade uppgifter ska vara underställt strikta säkerhetsbestämmelser.

2. Uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED får inom EU överlämnas personligen av bidragsmottagarens personal om följande krav är uppfyllda:

a) De kuvert eller förpackningar som används ska vara ogenomskinliga och får inte ange att innehållet är säkerhetsskyddsklassificerat.

b) De säkerhetsskyddsklassificerade uppgifterna får inte lämna bärarens besittning.

c) Kuvertet eller förpackningen får inte öppnas *på vägen*.

3. När uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska vidarebefordras inom en medlemsstat genom personligt överlämnande via bidragsmottagarens personal ska detta överenskommas i förväg mellan det sändande och det mottagande verksamhetsstället. Den myndighet eller det verksamhetsställe som är avsändare ska informera den myndighet eller det verksamhetsställe som är mottagare om försändelsens närmare detaljer, däribland referens, klassificering, förväntad ankomsttid och kurirens namn. Personligt överlämnande är tillåtet om följande krav är uppfyllda:

a) De säkerhetsskyddsklassificerade uppgifterna ligger i dubbla kuvert eller förpackningar.

b) Det yttre kuvertet eller förpackningsmaterialet ska vara säkrat och får inte ange att innehållet är säkerhetsskyddsklassificerat, medan det inre kuvertet ska vara märkt med relevant säkerhetsskyddsklassificeringsnivå.

c) De säkerhetsskyddsklassificerade EU-uppgifterna får inte lämna bärarens besittning.

d) Kuvertet eller förpackningen får inte öppnas *på vägen*.

e) Kuvertet eller förpackningen ska befordras i låsbar portfölj eller liknande godkänd väska av sådan storlek och vikt att bäraren hela tiden kan bära den med sig utan att behöva lämna den i bagageutrymme.

f) Kuriren ska vara försedd med kuririntyg utfärdat av dennes behöriga säkerhetsmyndighet vilket ger kuriren behörighet att överlämna den angivna säkerhetsklassade försändelsen.

([11]) Minimikraven för kommunikations- och informationssystem som används för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED fastställs i tillägg E i bilaga III.

([12]) Kommissionens beslut (EU, Euratom) 2019/1962 av den 17 oktober 2019 om genomförandebestämmelser för hantering av EU-uppgifter på säkerhetsskyddsklassificeringsnivån RESTREINT UE/EU RESTRICTED (EUT L 311, 2.12.2019, s. 21).

([13]) Kommissionens beslut (EU, Euratom) 2019/1961 av den 17 oktober 2019 om genomförandebestämmelser för hantering av EU-uppgifter på säkerhetsskyddsklassificeringsnivåerna CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET (EUT L 311, 2.12.2019, s. 1).

4. När uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska vidarebefordras från en medlemsstat till en annan genom personligt överlämnande via bidragsmottagarens personal ska följande tilläggsbestämmelser tillämpas:

a) Kuriren ska ansvara för det säkerhetsklassade materialets säkerhet till dess att det överlämnats till sin mottagare.

b) Vid överträdelser av säkerhetsbestämmelserna kan den avsändande nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten begära att myndigheterna i det land där överträdelsen ägde rum ska göra en utredning, rapportera sina resultat och vidta rättsliga eller andra lämpliga åtgärder.

c) Kuriren ska ha fått information om alla säkerhetsförpliktelser avseende överlämnandet och ska ha undertecknat en bekräftelse därom.

d) Instruktioner för kuriren ska bifogas kuririntyget.

e) Kuriren ska ha fått en beskrivning av försändelsen och en resväg.

f) Handlingarna ska återställas till den utfärdande nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten när resan avslutats eller hållas tillgängliga för tillsyn av mottagaren.

g) Om tull, migrationsmyndigheter eller gränspolis ber att få undersöka och kontrollera försändelsen ska de få öppna och se tillräckliga delar av försändelsen för att kunna fastställa att den inte innehåller annat material än det som deklarerats.

h) Tullmyndigheterna bör uppmanas att beakta den officiella ställning som bärarens transportdokument och tillstånd har.

Om försändelsen öppnas av tullen ska detta göras utom synhåll för obehöriga och om möjligt i kurirens närvaro. Kuriren ska begära att försändelsen ska återförpackas och ska be de myndigheter som utfört kontrollen att återförsegla försändelsen och skriftligen bekräfta att den öppnats av dem.

5. När uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska vidarebefordras till tredjeland eller till en internationell organisation genom personligt överlämnande via bidragsmottagarens personal ska detta ske i enlighet med bestämmelserna i informationssäkerhetsavtalet eller den administrativa överenskommelse som ingåtts mellan unionen eller kommissionen och det berörda tredjelandet eller den berörda internationella organisationen.

KAPITEL 6

KONTINUITETSPLANERING

Artikel 16

Beredskapsplaner och återställande åtgärder

Den bidragsbeviljande myndigheten ska säkerställa att det i det säkerhetsskyddsklassificerade bidragsavtalet ställs krav på att bidragsmottagaren ska ha en beredskapsplan för att vid nödsituationer skydda säkerhetsskyddsklassificerade EU-uppgifter som hanteras inom ramen för det säkerhetsskyddsklassificerade bidraget och att inom ramen för sin kontinuitetsplan inrätta förebyggande och återställande åtgärder för att minimera verkningarna av incidenter i samband med hantering och lagring av säkerhetsskyddsklassificerade EU-uppgifter. Bidragsmottagarna ska bekräfta för den bidragsbeviljande myndigheten att de har beredskapsplaner på plats.

Artikel 17

Ikraftträdande

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

Utfärdat i Bryssel den 10 februari 2021.

På kommissionens vägnar
För ordföranden
Johannes HAHN
Ledamot av kommissionen

BILAGA I

STANDARDINFORMATION I INBJUDAN

(bör anpassas till den inbjudan som används)

Säkerhet

Projekt som involverar säkerhetsskyddsklassificerade EU-uppgifter måste genomgå en säkerhetskontroll för godkännande av finansiering och kan komma att omfattas av specifika säkerhetsbestämmelser (som anges i säkerhetsskyddsöverenskommelse som bifogas bidragsavtalet).

I dessa bestämmelser (som styrs genom kommissionens beslut (EU, Euratom) 2015/444 ([1]) och/eller nationella regler) föreskrivs exempelvis följande:

— Projekt som involverar uppgifter som säkerhetsskyddsklassificerats som TRES SECRET UE/EU TOP SECRET (eller motsvarande) kan **INTE** erhålla medel.

— Säkerhetsskyddsklassificerade uppgifter ska markeras i enlighet med tillämpliga säkerhetsinstruktioner i säkerhetsskyddsöverenskommelsen.

— Uppgifter som säkerhetsskyddsklassificerats som minst CONFIDENTIEL UE/EU CONFIDENTIAL (och RESTREINT UE/EU RESTRICTED om så krävs enligt nationella regler) får

  — endast skapas och tillgås i lokaler med säkerhetsgodkännande av verksamhetsställe från den behöriga nationella säkerhetsmyndigheten, i enlighet med de nationella reglerna,

  — endast hanteras i ett säkrat utrymme som ackrediterats av en behörig nationell säkerhetsmyndighet,

  — endast bedömas och hanteras av personer med ett giltigt personalsäkerhetsgodkännande och behovsenlig behörighet.

— I bidragets slutskede ska de säkerhetsskyddsklassificerade uppgifterna antingen återlämnas eller fortsättningsvis skyddas i enlighet med tillämpliga bestämmelser.

— Uppgifter som inbegriper säkerhetsskyddsklassificerade EU-uppgifter kan endast läggas ut på underentreprenad med skriftligt förhandsgodkännande från den bidragsbeviljande myndigheten och endast till personer som är registrerade i en EU-medlemsstat eller i ett tredjeland med ett informationssäkerhetsavtal med EU (eller en administrativ överenskommelse med kommissionen).

— Röjande av säkerhetsskyddsklassificerade EU-uppgifter för tredje man kräver skriftligt förhandsgodkännande från den bidragsbeviljande myndigheten.

Observera att säkerhetsgodkännande av verksamhetsställe kan behöva tillhandahållas innan avtalet undertecknas, beroende på typen av verksamhet. Den bidragsbeviljande myndigheten kommer att bedöma behovet av godkännande i varje enskilt fall och fastställa deras leveransdatum under förberedandet av bidraget. Observera att vi under **inga omständigheter** kan underteckna något bidragsavtal förrän minst en av bidragsmottagarna i ett konsortium har erhållit säkerhetsgodkännande av verksamhetsställe.

Ytterligare säkerhetsrekommendationer kan läggas till i bidragsavtalet i form av säkerhetspunkter (*t.ex. inrättade av rådgivande säkerhetsgrupp, begränsning av detaljnivån, användning av falska scenarier, uteslutning av användning av säkerhetsskyddsklassificerade uppgifter, etc.*).

Bidragsmottagarna måste säkerställa att deras projekt inte omfattas av nationella säkerhetskrav eller säkerhetskrav från tredjeländer som skulle kunna påverka genomförandet eller ifrågasätta tilldelningen av bidraget (*t.ex. tekniska begränsningar, nationell säkerhetsklassificering, etc.*). Den bidragsbeviljande myndigheten måste underrättas omedelbart om eventuella säkerhetsfrågor.

[ytterligare MÖJLIGHET för ramavtal om partnerskap: Vid rampartnerskap ska både rampartnerskapsansökningarna och bidragsansökningarna genomgå en säkerhetskontroll.]

([1]) Se kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

BILAGA II

STANDARDKLAUSULER FÖR BIDRAGSAVTAL

(bör anpassas till det bidragsavtal som används)

13.2 Säkerhet – säkerhetsskyddsklassificerade uppgifter

Parterna ska hantera säkerhetsskyddsklassificerade uppgifter (EU-uppgifter eller nationella uppgifter) i enlighet med tillämplig EU-lagstiftning eller nationell lagstiftning om säkerhetsskyddsklassificerade uppgifter (särskilt kommissionens beslut (EU, Euratom) 2015/444 ([1]) och dess genomförandebestämmelser).

Särskilda säkerhetsbestämmelser (om sådana finns) fastställs i bilaga 5.

BILAGA 5

Säkerheten – säkerhetsskyddsklassificerade EU-uppgifter

[MÖJLIGHET för åtgärder som inbegriper säkerhetsskyddsklassificerade EU-uppgifter (standard): Om åtgärden medför användning eller generering av säkerhetsskyddsklassificerade EU-uppgifter ska uppgifterna behandlas i enlighet med handboken om säkerhetsklassificering och säkerhetsskyddsöverenskommelsen i bilaga 1 samt beslut (EU, Euratom) 2015/444 och dess tillämpningsföreskrifter, till dess att uppgifterna inte längre är säkerhetsskyddsklassificerade.

Resultat som innehåller säkerhetsskyddsklassificerade EU-uppgifter ska lämnas in enligt särskilda förfaranden som överenskommits med den bidragsbeviljande myndigheten.

Uppgifter som inbegriper säkerhetsskyddsklassificerade EU-uppgifter kan endast läggas ut på underentreprenad med uttryckligt skriftligt förhandsgodkännande från den bidragsbeviljande myndigheten och endast till personer som är registrerade i en EU-medlemsstat eller i ett tredjeland med ett informationssäkerhetsavtal med EU (eller en administrativ överenskommelse med kommissionen).

Säkerhetsskyddsklassificerade EU-uppgifter får inte röjas för tredje man (inte heller deltagare i genomförandet av åtgärden) utan skriftligt förhandsgodkännande från den bidragsbeviljande myndigheten.]

([1]) Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

BILAGA III

[Bilaga IV (till ……)]

SÄKERHETSSKYDDSÖVERENSKOMMELSE [1]

[Mall]

[1] Denna mall för säkerhetsskyddsöverenskommelse gäller där kommissionen anses som upphovsman till de säkerhetsskyddsklassificerade uppgifter som skapas eller hanteras i samband med fullgörandet av bidragsavtalet. Om upphovsmannen till de säkerhetsskyddsklassificerade uppgifter som skapas eller hanteras i samband med fullgörandet av bidragsavtalet inte är kommissionen och om en specifik säkerhetsram upprättas av de medlemsstater som deltar i bidraget kan andra mallar för säkerhetsskyddsöverenskommelse vara tillämpliga.

Tillägg A

SÄKERHETSKRAV

Den bidragsbeviljande myndigheten ska ta med följande säkerhetsbestämmelser i säkerhetsskyddsöverenskommelsen. Vissa av klausulerna kanske inte är tillämpliga på bidragsavtalet. Dessa anges inom hakparentes.

Förteckningen över klausuler är icke uttömmande. Ytterligare klausuler får läggas till beroende på vilken typ av säkerhetsskyddsklassificerade bidrag det är fråga om.

ALLMÄNNA VILLKOR [*OBS: gäller för alla säkerhetsskyddsklassificerade bidragsavtal*]

1. Denna säkerhetsskyddsöverenskommelse är en integrerad del av det säkerhetsskyddsklassificerade bidragsavtalet [eller underentreprenörsavtal] som kräver säkerhetsavtal och beskriver specifika säkerhetskrav för bidragsavtalet. Om kraven inte fullgörs kan detta utgöra tillräckliga skäl för uppsägning av bidragsavtalet.

2. Bidragsmottagare är underställda alla skyldigheter som fastställs i kommissionens beslut (EU, Euratom) 2015/444 ([2]) och dess tillämpningsföreskrifter ([3]). Om bidragsmottagaren stöter på problem i samband med tillämpningen av tillämpliga rättslig ram i en medlemsstat ska den hänvisa till kommissionens säkerhetsmyndighet och den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten.

3. Säkerhetsskyddsklassificerade uppgifter som genereras vid fullgörandet av bidragsavtalet ska märkas som säkerhetsskyddsklassificerade EU-uppgifter på lämplig säkerhetsnivå i enlighet med handboken om säkerhetsklassificering i bilaga B till denna säkerhetsskyddsöverenskommelse. Avvikelse från de säkerhetsskyddsnivåer som anges i handboken om säkerhetsklassificering är tillåten endast med skriftligt tillstånd från den bidragsbeviljande myndigheten.

4. De rättigheter som tillkommer upphovsmannen till säkerhetsskyddsklassificerade EU-uppgifter som skapas och hanteras i samband med fullgörandet av bidragsavtal som kräver säkerhetsavtal ska tillfalla kommissionen i egenskap av bidragsbeviljande myndighet.

5. Utan skriftligt tillstånd från den bidragsbeviljande myndigheten får bidragsmottagaren eller underentreprenören inte använda några uppgifter eller något material som tillhandahållits av den bidragsbeviljande myndigheten eller som framställts för dess räkning i andra syften än de som anges i bidragsavtalet.

6. Om säkerhetsgodkännande av verksamhetsställe krävs för fullgörandet av ett bidragsavtal ska bidragsmottagaren be den bidragsbeviljande myndigheten att fortsätta med begäran om säkerhetsgodkännande av verksamhetsställe.

7. Bidragsmottagaren är skyldig att utreda alla överträdelser av säkerhetsbestämmelserna som avser säkerhetsskyddsklassificerade EU-uppgifter och rapportera dem till den bidragsbeviljande myndigheten så snart detta är möjligt. Bidragsmottagaren eller underentreprenören ska omedelbart till sin ansvariga nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet samt, när detta är tillåtet enligt nationella lagar och andra föreskrifter, till kommissionens säkerhetsmyndighet rapportera alla situationer där det fastställts eller finns skäl att misstänka att säkerhetsskyddsklassificerade EU-uppgifter som tillhandahållits eller genererats i anknytning till bidragsavtalet har förkommit eller yppats för obehöriga.

([2]) Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53).

([3]) Den bidragsbeviljande myndigheten bör föra in hänvisningarna när tillämpningsföreskrifterna har antagits.

8. När bidragsavtalet löpt ut ska bidragsmottagaren eller underentreprenören återsända alla säkerhetsskyddsklassificerade EU-uppgifter i deras besittning till den bidragsbeviljande myndigheten så snart som möjligt. Bidragsmottagaren eller underentreprenören får, om detta är möjligt, förstöra de säkerhetsskyddsklassificerade EU-uppgifterna istället för att återsända dem. Detta ska ske i enlighet med nationella lagar och andra föreskrifter i det land där bidragsmottagaren har sitt säte, med förhandstillstånd från kommissionens säkerhetsmyndighet och enligt den myndighetens instruktioner. Säkerhetsskyddsklassificerade EU-uppgifter ska förstöras på ett sådant sätt att de inte kan återskapas, vare sig helt eller delvis.

9. Om bidragsmottagaren eller underentreprenören har rätt att behålla säkerhetsskyddsklassificerade EU-uppgifter när bidragsavtalet fullgjorts eller avslutats måste uppgifterna fortsätta skyddas i enlighet med beslut (EU, Euratom) 2015/444 och dess tillämpningsföreskrifter ([4]).

10. All elektronisk hantering, behandling och överföring av säkerhetsskyddsklassificerade EU-uppgifter måste ske enligt de bestämmelser som fastställs i kapitel 5 och 6 i kommissionens beslut 2015/444. Detta omfattar bland annat krav på att de kommunikations- och informationssystem som ägs av en bidragsmottagare och som används för att hantera säkerhetsskyddsklassificerade EU-uppgifter vid fullgörandet av bidragsavtalet (nedan kallat *bidragsmottagarens kommunikations- och informationssystem*) ska vara ackrediterat ([5]). All elektronisk överföring av säkerhetsskyddsklassificerade EU-uppgifter ska skyddas av kryptoprodukter som är godkända enligt artikel 36.4 i kommissionens beslut 2015/444 och tempestsäkerhetsåtgärder ska genomföras i enlighet med artikel 36.6 i kommissionens beslut 2015/444.

11. Bidragsmottagaren eller underentreprenören ska ha beredskapsplaner för att vid nödsituationer skydda säkerhetsskyddsklassificerade EU-uppgifter som hanteras i samband med fullgörandet av det säkerhetsskyddsklassificerade bidragsavtalet och ska vidta förebyggande och återställande åtgärder för att minimera följderna av incidenter vid hantering och lagring av säkerhetsskyddsklassificerade EU-uppgifter. Bidragsmottagaren eller underentreprenören ska informera den bidragsbeviljande myndigheten om sin beredskapsplan.

BIDRAGSAVTAL DÄR TILLGÅNG KRÄVS TILL UPPGIFTER SOM SÄKERHETSKLASSATS PÅ NIVÅN RESTREINT UE/EU RESTRICTED

12. Personalsäkerhetsgodkännande krävs i princip inte för fullgörande av bidragsavtalet ([6]). Men uppgifter och material som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED får bara vara tillgängliga för den personal hos bidragsmottagaren som behöver dem för att kunna fullgöra bidragsavtalet (*principen om behovsenlig behörighet*) och som informerats av bidragsmottagarens säkerhetsansvariga om sina skyldigheter och om följderna av eventuella läckor eller överträdelser av säkerhetsbestämmelserna, och som skriftligen bekräftat att de informerats om följderna av bristande skydd av säkerhetsskyddsklassificerade EU-uppgifter.

13. Utan skriftligt medgivande från den bidragsbeviljande myndigheten får bidragsmottagaren och underentreprenören inte ge tillgång till uppgifter eller material som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED till någon annan enhet eller person än anställda med behovsenlig behörighet.

14. Bidragsmottagaren eller underentreprenören måste låta säkerhetskoderna stå kvar på säkerhetsskyddsklassificerade uppgifter som genererats eller tillhandahållits i samband med fullgörandet av bidragsavtalet och får inte deklassificera uppgifter utan skriftligt tillstånd från den bidragsbeviljande myndigheten.

15. Uppgifter och material som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED ska förvaras i låsbara kontorsmöbler när de inte används. Handlingar måste förvaras i ogenomskinligt kuvert under transport. Handlingar får inte lämna bärarens besittning och får inte öppnas *under transporten*.

([4]) Den bidragsbeviljande myndigheten bör föra in hänvisningarna när tillämpningsföreskrifterna har antagits.

([5]) Den part som åtar sig att göra säkerhetsackreditering måste förse den bidragsbeviljande myndigheten med ett överensstämmelseintyg, via kommissionens säkerhetsmyndighet, i samförstånd med den berörda nationella ackrediteringsmyndigheten för säkerhet.

([6]) Om bidragsmottagarna kommer från medlemsstater som kräver personalsäkerhetsgodkännande och/eller säkerhetsgodkännande av verksamhetsställe för bidrags som säkerhetsskyddsklassificerats på nivån RESTREINT UE/EU RESTRICTED ska den bidragsbeviljande myndigheten ange kraven avseende personalsäkerhetsgodkännande och säkerhetsgodkännande av verksamhetsställe för de berörda bidragsmottagarna i säkerhetsskyddsöverenskommelsen.

16. Bidragsmottagaren eller underentreprenören får översända handlingar som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED till den bidragsbeviljande myndigheten med kommersiella kurirtjänster, per post, genom personligt överlämnande eller elektroniskt. I detta syfte ska bidragsmottagaren och underentreprenören följa kommissionens säkerhetsanvisningar för program eller projekt och/eller kommissionens tillämpningsföreskrifter för industrisäkerhet avseende säkerhetsskyddsklassificerade bidrag ([7]).

17. När de inte längre behövs ska handlingar som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED förstöras på ett sådant sätt att de inte kan återskapas, vare sig helt eller delvis.

18. Säkerhetsackreditering av bidragsmottagarens kommunikations- och informationssystem för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED och all sammankoppling av sådana system får delegeras till bidragsmottagarens säkerhetsansvariga om detta är tillåtet enligt nationella lagar och andra föreskrifter. När ackreditering delegeras behåller dock de berörda nationella säkerhetsmyndigheterna, utsedda säkerhetsmyndigheterna och ackrediteringsmyndigheterna för säkerhet ansvaret för att skydda uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED som hanteras av bidragsmottagaren och ska ha rätt att inspektera bidragsmottagarens säkerhetsåtgärder. Bidragsmottagaren ska därutöver förse den bidragsbeviljande myndigheten, och där så krävs enligt nationella lagar och andra föreskrifter även den behöriga nationella ackrediteringsmyndigheten för säkerhet, med ett överensstämmelseintyg som styrker att bidragsmottagarens kommunikations- och informationssystem och därmed sammankopplade system har ackrediterats för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED.

HANTERING AV UPPGIFTER SOM SÄKERHETSKLASSATS PÅ NIVÅN RESTREINT UE/EU RESTRICTED I KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

19. Minimikraven för kommunikations- och informationssystem för hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED fastställs i tillägg E till denna säkerhetsskyddsöverenskommelse.

FÖRUTSÄTTNINGAR DÅ BIDRAGSMOTTAGAREN FÅR ANVÄNDA SIG AV UNDERENTREPRENAD

20. Bidragsmottagaren måste erhålla tillstånd från den bidragsbeviljande myndigheten innan någon del av det säkerhetsskyddsklassificerade bidragsavtalet läggs ut på underentreprenad.

21. Ingen underentreprenad får beviljas personer som är registrerade i tredjeland eller enheter som tillhör internationella organisationer, om inte det aktuella tredjelandet eller den internationella organisationen ingått ett informationssäkerhetsavtal med EU eller en administrativ överenskommelse med kommissionen.

22. Om bidragsmottagaren använt underentreprenad ska säkerhetsbestämmelserna i bidragsavtalet *i tillämpliga delar* omfatta även underentreprenören och dennes personal. Det åligger då bidragsmottagaren att se till att alla underentreprenörer tillämpar samma principer på sina överenskommelser. För att garanteras lämplig säkerhetstillsyn ska kommissionens säkerhetsmyndighet underrätta bidragsmottagarens och underentreprenörens nationella säkerhetsmyndighet och/eller utsedda säkerhetsmyndighet om tilldelning av alla relaterade underentreprenörsavtal på nivån CONFIDENTIEL UE/EU CONFIDENTIAL och SECRET UE/EU SECRET. Vid behov ska bidragsmottagarens och underentreprenörens nationella säkerhetsmyndighet och/eller utsedda säkerhetsmyndighet förses med en kopia av de säkerhetsbestämmelser som specifikt gäller underentreprenaden. De nationella säkerhetsmyndigheter och utsedda säkerhetsmyndigheter som ska underrättas om säkerhetsbestämmelserna i säkerhetsskyddsklassificerade bidragsavtal som kräver säkerhetsavtal på nivån RESTREINT UE/EU RESTRICTED förtecknas i bilagan till kommissionens tillämpningsföreskrifter för industrisäkerhet avseende säkerhetsskyddsklassificerade bidragsavtal ([8]).

23. Bidragsmottagaren får inte lämna ut säkerhetsskyddsklassificerade EU-uppgifter till underentreprenörer utan skriftligt förhandstillstånd från den bidragsbeviljande myndigheten. Om säkerhetsskyddsklassificerade EU-uppgifter ska överlämnas till underentreprenörer ofta eller rutinmässigt får den bidragsbeviljande myndigheten lämna tillstånd för viss tid (t.ex. 12 månader) eller för underentreprenörsavtalets löptid.

([7]) Den bidragsbeviljande myndigheten bör föra in hänvisningarna när tillämpningsföreskrifterna har antagits.
([8]) Den bidragsbeviljande myndigheten bör föra in hänvisningarna när tillämpningsföreskrifterna har antagits.

BESÖK

Om det sedvanliga förfarandet för begäran om besök ska tillämpas på besök som medför tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska den bidragsbeviljande myndigheten ta med punkterna 24, 25 och 26 samt stryka punkt 27. Om besök som medför tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET anordnas gemensamt av det sändande och det mottagande verksamhetsstället ska den bidragsbeviljande myndigheten stryka punkterna 25 och 26 och endast ta med punkt 27.

24. Besök som medför eller som kan medföra tillgång till uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED ska anordnas gemensamt av det sändande och det mottagande verksamhetsstället utan att förfarandet i punkterna 25–27 nedan behöver följas.

[25. Besök som medför eller som kan medföra tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska ske enligt följande förfarande:

a) Den säkerhetsansvariga på det verksamhetsställe som sänder ut besökaren ska fylla i alla relevanta delar av formuläret för begäran om besök (tillägg C) och lämna begäran till verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet.

b) Det sändande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet ska bekräfta besökarens personalsäkerhetsgodkännande innan begäran om besök lämnas till det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet (eller kommissionens säkerhetsmyndighet om besöket sker i den bidragsbeviljande myndighetens lokaler).

c) Den säkerhetsansvariga vid det sändande verksamhetsstället ska därefter från sin nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet inhämta det svar som lämnats av det mottagande verksamhetsställets nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet (eller av kommissionens säkerhetsmyndighet) varigenom begäran om besök antingen beviljas eller avslås.

d) En begäran om besök anses godkänd om inga invändningar görs fram till fem dagar innan besöket.]

[26. Innan besökaren eller besökarna får tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska det mottagande verksamhetsstället invänta tillstånd från sin nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet.]

[27. Besök som medför eller kan medföra tillgång till uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET ska anordnas gemensamt av det sändande och det mottagande verksamhetsstället (ett exempel på formulär som kan användas finns i tillägg C).]

28. Besökarna ska styrka sin identitet när de anländer till det mottagande verksamhetsstället genom att uppvisa giltig ID-handling eller pass.

29. Det verksamhetsställe som tar emot besök ska säkerställa att alla besökare registreras. Uppgifterna ska omfatta besökarnas namn, den organisation de företräder, sista giltighetsdag för deras personalsäkerhetsgodkännande (i förekommande fall), besöksdatum och namnet på de besökta personerna. Utan att det hindrar tillämpningen av EU:s bestämmelser om dataskydd får dessa register sparas under minst fem år eller under den tid som fastställs i nationella lagar och andra föreskrifter, beroende på vad som är lämpligast.

UTVÄRDERINGSBESÖK

30. Kommissionens säkerhetsmyndighet får i samråd med den berörda nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten göra besök på bidragsmottagares eller underentreprenörers verksamhetsställen för att kontrollera att säkerhetskraven för hantering av säkerhetsskyddsklassificerade EU-uppgifter är uppfyllda.

HANDBOK OM SÄKERHETSKLASSIFICERING

31. En förteckning över alla inslag i bidragsavtalet som är säkerhetsskyddsklassificerade eller ska säkerhetsskyddsklassificeras i samband med bidragsavtalets fullgörande, bestämmelserna för detta och angivande av tillämpliga klassificeringsnivåer finns i handboken om säkerhetsklassificering. Handboken om säkerhetsklassificering utgör en integrerad del av detta bidragsavtal och finns i tillägg B till denna bilaga.

Tillägg B

HANDBOK OM SÄKERHETSKLASSIFICERING

[Lydelsen bör justeras i förhållande till föremålet för bidragsavtalet]

Tillägg C

BEGÄRAN OM BESÖK (MALL)

NÄRMARE ANVISNINGAR FÖR IFYLLANDE AV BEGÄRAN OM BESÖK

(Ansökan måste lämnas på engelska)

RUBRIK	Kryssa för de rutor som är tillämpliga på besöket och uppgifterna och ange antal platser som ska besökas och antal besökare.
4. **ADMINISTRATIVA UPPGIFTER**	Ska fyllas i av den begärande nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten.
5. **BEGÄRANDE ORGANISATION ELLER INDUSTRIELL ANLÄGGNING**	Ange fullständigt namn och fullständig postadress. Ange ort, postnummer och i förekommande fall region.
6. **ORGANISATION ELLER INDUSTRIELL ANLÄGGNING SOM SKA BESÖKAS**	Ange fullständigt namn och fullständig postadress. Ange ort, region, postnummer, telex eller faxnummer (om sådant finns), telefonnummer och e-post. Lämna namn och telefon- eller faxnummer samt e-postadress till den ansvariga kontaktpersonen eller den person som bokat in besöket. Anmärkningar: 1) Det är viktigt att postnumret är korrekt eftersom samma företag kan ha flera olika verksamhetsställen. 2) Vid manuell ansökan kan bilaga 1 användas om två eller flera verksamhetsställen ska besökas av samma anledning. Om en bilaga används ange följande i punkt 3: ”SE BILAGA 1, ANTAL VERKSAMHETSSTÄLLEN: ...” (ange antal verksamhetsställen)
7. **BESÖKSDAG**	Lämna uppgift om faktisk besöksdag eller besöksperiod (inledningsdatum och slutdatum) i formatet ”dag - månad - år”. Ange i förekommande fall andra datum och perioder inom hakparentes.
8. **TYP AV INITIATIV**	Ange om besöket sker på den begärande organisationens eller verksamhetsställets initiativ eller på inbjudan från det verksamhetsställe som ska besökas.
9. **BESÖKET ANGÅR**	Lämna en fullständig hänvisning till projektet, kontraktet eller inbjudan att lämna förslag och använd endast vedertagna förkortningar.
10. **ÄMNE SOM SKA DISKUTERAS/ MOTIVERING**	Lämna en kortfattad beskrivning av skälet eller skälen till besöket. Använd inte förkortningar utan förklaring. Anmärkningar: Vid återkommande besök bör detta anges här (t.ex. ”Återkommande besök för att diskutera _____”).
11. **BERÄKNAD SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅ FÖR DEN INFORMATION SOM AVSES**	Ange SECRET UE/EU SECRET (S-UE/EU-S) eller CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), beroende på vad som är lämpligt.

12. **UPPGIFTER OM BESÖKAREN**	Anmärkning: Om fler än två personer avlägger besök används bilaga 2.
13. **DEN BEGÄRANDE ENHETENS SÄKERHETSANSVARIGE**	Ange namn, telefonnummer, faxnummer och e-post till den begärande enhetens säkerhetsansvariga.
14. **CERTIFIERING AV SÄKERHETSGODKÄNNANDE**	Ska fyllas i av den intygande myndigheten. Anmärkningar avseende den intygande myndigheten: a. Ange namn, adress, telefonnummer, faxnummer och e-postadress (får vara förtryckt). b. Denna punkt ska förses med namnteckning och stämpel (i förekommande fall).
15. **BEGÄRANDE SÄKERHETSMYNDIGHET**	Ska fyllas i av den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten. Anmärkningar avseende den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten: a. Ange namn, adress, telefonnummer, faxnummer och e-postadress (får vara förtryckt). b. Denna punkt ska förses med namnteckning och stämpel (i förekommande fall).

Alla fält ska fyllas i och formuläret översändas via kanaler för kommunikation mellan regeringar ([9]).

BEGÄRAN OM BESÖK

(MALL)

BEGÄRAN STÄLLS TILL: _____

1. **TYP AV BESÖK**	2. **TYP AV INFORMATION**	3. **SAMMANFATTNING**
☐ Enskilt ☐ Återkommande ☐ Nödsituation ☐ Ändring ☐ Datum ☐ Besökare ☐ Anläggning För ändring, ange den nationella säkerhetsmyndighetens/utsedda säkerhetsmyndighetens ursprungliga referensnummer för begäran om besök_____	☐ C-UE/EU-C ☐ S-UE/EU-S	Antal platser: _____ Antal besökare: _____

4. **ADMINISTRATIVA UPPGIFTER:**	
Begärande: Begäran ställs till:	Den nationella säkerhetsmyndighetens/utsedda säkerhetsmyndighetens referensnummer för begäran om besök_____ Datum *(dd/mm/åååå)*: _____/_____/_____

([9]) Om det är tillåtet att gemensamt anordna besök som kommer att eller kan medföra tillgång till säkerhetsskyddsklassificerade EU-uppgifter på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET får det ifyllda formuläret lämnas direkt till den säkerhetsansvariga vid den inrättning som ska besökas.

5. **BEGÄRANDE ORGANISATION ELLER INDUSTRIELL ANLÄGGNING**

NAMN:

POSTADRESS:

E-POSTADRESS:

FAX:— TELEFON:

6. **ORGANISATION(ER) ELLER INDUSTRIELL(A) ANLÄGGNING(AR) SOM SKA BESÖKAS *(bilaga 1 ska fyllas i)***

7. **BESÖKSDAG *(dd/mm/åååå)*: FRÅN _____/_____/_____ TILL _____/_____/_____**

8. **TYP AV INITIATIV:**

☐ Inleds av begärande organisation eller anläggning

☐ Genom inbjudan från den anläggning som ska besökas:

9. **BESÖKET AVSER KONTRAKT:**

10. **ÄMNE SOM SKA DISKUTERAS/SKÄL/SYFTE (Inkludera uppgifter om värdenheten samt annan relevant information. Förkortningar bör undvikas):**

–11. **BERÄKNAD HÖGSTA SÄKERHETSSKYDDSKLASSIFICERINGSNIVÅ FÖR DEN INFORMATION/DET MATERIAL ELLER DET ANLÄGGNINGSTILLTRÄDE SOM AVSES:**

12. **UPPGIFTER OM BESÖKARE *(bilaga 2 ska fyllas i)*:**

13. **DEN BEGÄRANDE ORGANISATIONENS ELLER INDUSTRIELLA ANLÄGGNINGENS SÄKERHETSANSVARIGE:**

NAMN:

TELEFON:

E-POSTADRESS:

UNDERSKRIFT:

14. CERTIFIERING AV NIVÅ PÅ SÄKERHETSGODKÄNNANDE:

NAMN:

ADRESS:

TELEFON:

E-POSTADRESS:

UNDERSKRIFT:

STÄMPEL

DATUM *(dd/mm/åååå)*:
_____/_____/_____

15. **BEGÄRANDE NATIONELL SÄKERHETSMYNDIGHET/UTSEDD SÄKERHETSMYNDIGHET:** NAMN: ADRESS: TELEFON: E-POSTADRESS: UNDERSKRIFT: STÄMPEL DATUM *(dd/mm/åååå)*: _____/_____/_____
16. **ANMÄRKNINGAR *(obligatorisk motivering krävs vid brådskande besök)*:**

<För in hänvisning till tillämplig lagstiftning om personuppgifter och en länk till obligatoriska upplysningar till den registrerade, t.ex. om tillämpningen av artikel 13 i den allmänna dataskyddsförordningen ([10]).>

([10]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

BILAGA 1 till FORMULÄRET FÖR BEGÄRAN OM BESÖK

ORGANISATION(ER) ELLER INDUSTRIELL(A) ANLÄGGNING(AR) SOM SKA BESÖKAS
1. NAMN: ADRESS: TELEFON: FAX: KONTAKTPUNKTENS NAMN: E-POST: TELEFON: NAMNET PÅ DEN SÄKERHETSANSVARIGA ELLER DEN SEKUNDÄRA KONTAKTPUNKTEN: E-POST: TELEFON:
2. NAMN: ADRESS: TELEFON: FAX: KONTAKTPUNKTENS NAMN: E-POST: TELEFON: NAMNET PÅ DEN SÄKERHETSANSVARIGA ELLER DEN SEKUNDÄRA KONTAKTPUNKTEN: E-POST: TELEFON: ***(fortsätt enligt behov)***

<För in hänvisning till tillämplig lagstiftning om personuppgifter och en länk till obligatoriska upplysningar till den registrerade, t.ex. om tillämpningen av artikel 13 i den allmänna dataskyddsförordningen ([11]).>

([11]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

BILAGA 2 till FORMULÄRET FÖR BEGÄRAN OM BESÖK

BESÖKARES KONTAKTUPPGIFTER
1. EFTERNAMN: FÖRNAMN *(enligt pass)*: FÖDELSEDATUM *(dd/mm/åååå)*:____/____/____ FÖDELSEORT: MEDBORGARSKAP: NIVÅ PÅ SÄKERHETSGODKÄNNANDE: PP-/ID-nummer BEFATTNING: FÖRETAG/ORGANISATION:
2. EFTERNAMN: FÖRNAMN *(enligt pass)*: FÖDELSEDATUM *(dd/mm/åååå)*:____/____/____ FÖDELSEORT: MEDBORGARSKAP: NIVÅ PÅ SÄKERHETSGODKÄNNANDE: PP-/ID-nummer BEFATTNING: FÖRETAG/ORGANISATION: ***(fortsätt enligt behov)***

<För in hänvisning till tillämplig lagstiftning om personuppgifter och en länk till obligatoriska upplysningar till den registrerade, t.ex. om tillämpningen av artikel 13 i den allmänna dataskyddsförordningen ([12]).>

([12]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

Tillägg D

INFORMATIONSBLAD FÖR SÄKERHETSGODKÄNNANDE AV VERKSAMHETSSTÄLLE (MALL)

1. **INLEDNING**

1.1 Nedan följer ett exempel på informationsblad för säkerhetsgodkännande av verksamhetsställe för snabbt informationsutbyte mellan nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter, andra behöriga nationella säkerhetsmyndigheter och kommissionens säkerhetsmyndighet (som handlar i egenskap av bidragsbeviljande myndigheter) när det gäller säkerhetsgodkännande av verksamhetsställe som berörs av ansökan om eller genomförandet av säkerhetsskyddsklassificerade bidrag eller underentreprenörsavtal.

1.2 Informationsbladet för säkerhetsgodkännande av verksamhetsställe är giltigt endast om det är stämplat av den nationella säkerhetsmyndigheten, utsedda säkerhetsmyndigheten eller en annan behörig myndighet.

1.3 Informationsbladet för säkerhetsgodkännande av verksamhetsställe är indelat i ett avsnitt för begäran och ett avsnitt för besvarande och kan användas för de ovannämnda syftena eller i andra fall då säkerhetsgodkännande av verksamhetsställe krävs. Skälet till begäran måste anges av den begärande nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten i fält 7.

1.4 Uppgifterna i informationsbladet för säkerhetsgodkännande av verksamhetsställe är i normalfallet inte säkerhetsskyddsklassificerade. När ett informationsblad för säkerhetsgodkännande av verksamhetsställe ska översändas mellan en nationell säkerhetsmyndighet, utsedd säkerhetsmyndighet eller kommissionen bör detta därför helst ske elektroniskt.

1.5 Nationella säkerhetsmyndigheter och utsedda säkerhetsmyndigheter bör göra sitt yttersta för att besvara ett informationsblad för säkerhetsgodkännande av verksamhetsställe inom tio arbetsdagar.

1.6 Om säkerhetsskyddsklassificerade uppgifter ska överföras eller ett bidragsavtal eller underentreprenörsavtal tilldelas med anledning av denna försäkran måste den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten informeras.

Förfarande och användningsinstruktioner avseende informationsbladet för säkerhetsgodkännande av verksamhetsställe

Dessa närmare instruktioner är avsedda för nationella säkerhetsmyndigheter, utsedda säkerhetsmyndigheter eller den bidragsbeviljande myndigheten och kommissionens säkerhetsmyndighet som ska fylla i informationsbladet för säkerhetsgodkännande av verksamhetsställe. Begäran bör fyllas i med versaler.

RUBRIK	Den begärande ska ange fullständigt namn på den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten med angivande av landsnamn.
1. **TYP AV BEGÄRAN**	Den bidragsbeviljande myndighet som gör begäran ska genom att kryssa i rutan ange vilken typ av begäran om informationsblad för säkerhetsgodkännande av verksamhetsställe som avses. Ange vilken säkerhetsnivå som avses. Följande förkortningar ska användas: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Kommunikations- och informationssystem för behandling av säkerhetsskyddsklassificerade uppgifter.
2. **UPPGIFTER OM DEN SÖKANDE**	Fält 1–6 är självförklarande. I fält 4 bör den sedvanliga landskoden med två bokstäver användas. Fält 5 är inte obligatoriskt.
3. **SKÄL TILL BEGÄRAN**	Ange skälen till begäran tillsammans med hänvisningar till projekt, numret på inbjudan eller bidraget. Ange behovet av lagringskapacitet, säkerhetsklassificeringsnivå på kommunikations- och informationssystem osv. Ange alla frister/löptider/tilldelningsdatum som kan vara av vikt för säkerhetsgodkännandet av verksamhetsställe.

4. **BEGÄRANDE NATIONELL SÄKERHETSMYNDIGHET ELLER UTSEDD SÄKERHETSMYNDIGHET**	Ange den faktiska sökandens namn (för vilken den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten agerar) och datum för begäran med siffror (dd/mm/åååå).
5. **SVARSDEL**	Fält 1–5: Fyll i lämpliga fält. Fält 2: Om ett säkerhetsgodkännande av verksamhetsställe är under behandling bör den begärande parten få preliminära uppgifter om beräknad behandlingstid (om denna är känd). Fält 6: a) Trots att valideringen varierar mellan länder och ibland till och med mellan verksamhetsställen är det rekommenderat att uppge ett slutdatum för säkerhetsgodkännandet av verksamhetsställe. b) Om inget slutdatum fastställts för säkerhetsgodkännande av verksamhetsställe får detta fält strykas. c) I enlighet med nationella lagar och andra föreskrifter ska endera den begärande parten eller bidragsmottagaren respektive underentreprenören vara ansvarig för att begära förnyat säkerhetsgodkännande av verksamhetsstället.
6. **ANMÄRKNINGAR**	Fältet kan användas för att lämna ytterligare upplysningar om säkerhetsgodkännandet, verksamhetsstället eller de föregående punkterna.
7. **UTFÄRDANDE NATIONELL SÄKERHETSMYNDIGHET ELLER UTSEDD SÄKERHETSMYNDIGHET**	Ange den utfärdande myndighetens namn (som agerar för den nationella säkerhetsmyndighetens eller utsedda säkerhetsmyndighetens räkning) och datum för svaret med siffror (dd/mm/åååå).

INFORMATIONSBLAD FÖR SÄKERHETSGODKÄNNANDE AV VERKSAMHETSSTÄLLE (MALL)

Alla fält ska fyllas i och formuläret översändas via kanaler för kommunikation mellan regeringar eller för kommunikation mellan regeringar och internationella organisationer.

BEGÄRAN OM INTYG OM SÄKERHETSGODKÄNNANDE AV VERKSAMHETSSTÄLLE

BEGÄRAN STÄLLS TILL: _____

(Land där den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten befinner sig)

Fyll i svarsfälten med nedanstående upplysningar i förekommande fall.

[ ] Begäran om tillhandahållande av säkerhetsgodkännande av verksamhetsställe på nivån: [ ] S-UE/EU-S [ ] C-UE/EU-C

för nedan angivna verksamhetsställe

[ ] och för lagring av material och uppgifter som säkerhetsklassificerats

[ ] och för kommunikations- och informationssystem (CIS) för behandling av säkerhetsskyddsklassificerade uppgifter

[ ] Begäran om att förfarande för att erhålla säkerhetsgodkännande av verksamhetsställe inleds, direkt eller på motsvarande begäran från en bidragsmottagare eller underentreprenör, till och med säkerhetsnivå ..... och för lagring säkerhetsnivå ..... samt för kommunikations- och informationssystem säkerhetsnivå ....., om verksamhetsstället inte redan har denna kapacitet.

Bekräfta riktigheten i nedanstående uppgifter om verksamhetsstället och gör vid behov korrigeringar eller tillägg.

1. Verksamhetsställets fullständiga namn: korrigering/tillägg:

....

2. Verksamhetsställets fullständiga adress:

....

3. Postadress (om annan än den som anges ovan):

....

4. Postnummer/ort/land:

....

5. Namn på den säkerhetsansvariga:

.....
.....

6. Telefon/fax/e-post till den säkerhetsansvariga:

....

7. Begäran görs av följande skäl: (lämna närmare upplysningar om stadiet innan kontraktstilldelning (urvalsförfarandet), bidrag eller underentreprenörsavtal, aktuellt program/projekt m.m.)

.....

Begärande nationell säkerhetsmyndighet, utsedd säkerhetsmyndighet eller bidragsbeviljande myndighet: Namn: .....

Datum: (dd/mm/åååå) .....

SVAR (inom tio arbetsdagar)

Härmed intygas följande:

1. [ ] Ovannämnda verksamhetsställe innehar säkerhetsgodkännande på nivån [ ] S-UE/EU-S

   [ ] C-UE/EU-C.

2. Ovannämnda verksamhetsställe har kapacitet att skydda uppgifter eller material som är säkerhetsskyddsklassificerade

   [ ] Ja, på nivå: ..... [ ] Nej

3. Ovannämnda verksamhetsställe har ett kommunikations- och informationssystem som är säkerhetsackrediterat eller godkänt

   [ ] Ja, på nivå: ..... [ ] Nej

4. [ ] Förfarandet för säkerhetsgodkännande av verksamhetsställe avseende ovanstående begäran har inletts. Ni kommer att informeras när säkerhetsgodkännandet meddelats eller vägrats.

5. [ ] Ovannämnda verksamhetsställe innehar inte säkerhetsgodkännande.

6. Detta säkerhetsgodkännande av verksamhetsställe upphör att gälla den ..... (*dd/mm/åååå*), eller enligt vad som anges av den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten. Om godkännandet återkallas dessförinnan eller ovanstående uppgifter ändras kommer ni att informeras.

7. Anmärkningar:
   .....

UTFÄRDANDE NATIONELL SÄKERHETSMYNDIGHET ELLER UTSEDD SÄKERHETSMYNDIGHET Namn:.....

Datum:(dd/mm/åååå).....

<För in hänvisning till tillämplig lagstiftning om personuppgifter och en länk till obligatoriska upplysningar till den registrerade, t.ex. om tillämpningen av artikel 13 i den allmänna dataskyddsförordningen ([13]).>

([13]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

Tillägg E

Minimikrav för skydd av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED som hanteras i elektronisk form i bidragsmottagarens kommunikations- och informationssystem

Allmänt

1. Bidragsmottagaren ska säkerställa att skyddet av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED uppfyller minimikraven i denna säkerhetsklausul och alla övriga krav som ställs av den bidragsbeviljande myndigheten eller i förekommande fall av den nationella säkerhetsmyndigheten eller utsedda säkerhetsmyndigheten.

2. Det är bidragsmottagaren som har ansvar för att genomföra säkerhetskraven i denna handling.

3. I denna handling avses med kommunikations- och informationssystem all utrustning som används för att hantera, lagra och överföra säkerhetsskyddsklassificerade EU-uppgifter, däribland arbetsstationer, skrivare, kopiatorer, faxapparater, servrar, näthanteringssystem, nätverkskort och kommunikationsstyrenheter, bärbara datorer, minidatorer, datorplattor, smarttelefoner och flyttbara minnen såsom USB-minnen, CD-skivor, SD-kort o.dyl.

4. Särskild utrustning, t.ex. kryptoprodukter, måste skyddas i enlighet med de därför avsedda säkra driftsmetoderna.

5. Bidragsmottagaren ska upprätta en struktur för säkerhetshantering i kommunikations- och informationssystem som används för hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED och ska utse en säkerhetsansvarig för det berörda verksamhetsstället.

6. Det är inte tillåtet för bidragsmottagarens personal att använda sin privata it-utrustning (maskinvara, programvara eller tjänster) för att lagra eller behandla uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED.

7. Säkerhetsackreditering av bidragsmottagarens kommunikations- och informationssystem för hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED ska godkännas av ackrediteringsmyndigheten för säkerhet i den berörda medlemsstaten eller delegeras till bidragsmottagarens säkerhetsansvariga om det är tillåtet enligt nationella lagar och andra föreskrifter.

8. Endast uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED som är krypterade med hjälp av godkända kryptoprodukter får hanteras, lagras eller överföras (via kabel eller trådlöst) på samma sätt som andra, icke säkerhetsskyddsklassificerade, uppgifter inom ramen för bidragsavtalet. Kryptoprodukterna måste ha godkänts av EU eller en medlemsstat.

9. Externa verksamhetsställen som arbetar med underhåll eller reparationer måste vara avtalsenligt bundna att följa tillämpliga bestämmelser om hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED enligt denna handling.

10. På begäran från den bidragsbeviljande myndigheten eller berörd nationell säkerhetsmyndighet/utsedd säkerhetsmyndighet/ackrediteringsmyndighet för säkerhet ska bidragsmottagaren styrka att denne uppfyller säkerhetsklausulen i bidragsavtalet. Om revision och kontroll av bidragsmottagarens rutiner och verksamhetsställen också begärs för att säkerställa efterlevnaden av dessa krav ska bidragsmottagaren tillåta att företrädare för den bidragsbeviljande myndigheten, den nationella säkerhetsmyndigheten, utsedda säkerhetsmyndigheten, ackrediteringsmyndigheten för säkerhet och/eller berörd säkerhetsmyndighet från EU utför sådan kontroll och revision.

Fysisk säkerhet

11. Områden där kommunikations- och informationssystemet används för att visa, lagra, behandla eller överföra uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED eller områden där servrar, näthanteringssystem, nätverkskort eller kommunikationsstyrenheter för sådana kommunikations- och informationssystem finns, bör inrättas som separata kontrollerade områden försedda med ett lämpligt system för kontroll av tillträdet. Tillträde till dessa separata och kontrollerade områden bör begränsas till personer med särskilt tillstånd. Utan att det hindrar tillämpningen av punkt 8, ska den utrustning som avses i punkt 3 lagras i separata och kontrollerade områden.

12. Säkerhetssystem och/eller säkerhetsrutiner ska tillämpas på införsel eller anslutning av flyttbara lagringsmedier för datorer (USB-minnen, masslagringsminnen eller omskrivningsbara CD:ar) till delar av kommunikations- och informationssystemet.

Tillgång till kommunikations- och informationssystem

13. Tillgång till bidragsmottagarens kommunikations- och informationssystem som hanterar säkerhetsskyddsklassificerade EU-uppgifter ska endast tillåtas för personal med vederbörligt tillstånd och behovsenlig behörighet.

14. Alla kommunikations- och informationssystem ska ha aktuella förteckningar över tillåtna användare. Användarautentisering ska göras i början av varje behandling.

15. Lösenord, som vanligen ingår i de säkerhetsåtgärder som används för identifiering och autentisering, ska innehålla minst nio tecken och måste bestå av såväl siffror och specialtecken (om systemet medger detta) som bokstäver. Lösenordet ska bytas efter högst 180 dagar. Lösenord ska bytas snarast om de har läckt eller lämnats ut till obehöriga, eller vid misstänkt läcka eller utlämning.

16. Alla kommunikations- och informationssystem ska vara försedda med interna tillgångskontroller för att hindra att obehöriga får tillgång till eller ändrar uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED eller ändrar systemen och säkerhetskontrollerna. Användare ska automatiskt loggas ut från kommunikations- och informationssystemet om terminalen varit inaktiv en viss förutbestämd tid; alternativt ska kommunikations- och informationssystemet aktivera en lösenordskyddad skärmsläckare efter 15 minuters inaktivitet.

17. Alla användare av kommunikations- och informationssystemet ska tilldelas ett unikt användarkonto och användarnamn. Användarkonton ska automatiskt låsas om minst fem misslyckade inloggningsförsök i rad görs.

18. Alla användare av kommunikations- och informationssystemet ska uppmärksammas på sina skyldigheter och de rutiner som ska följas för att skydda uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED i kommunikations- och informationssystemet. Skyldigheterna och rutinerna ska dokumenteras och användarna ska skriftligen bekräfta att de informerats.

19. Säkra driftsmetoder ska vara tillgängliga för användarna och administratörerna och ska omfatta beskrivningar av säkerhetsrollerna och därmed sammanhängande uppgifter, instruktioner och planer.

Redovisning, revision och incidenthantering

20. All tillgång till kommunikations- och informationssystem ska registreras i en logg.

21. Följande händelser ska registreras:

    a) Alla försök att logga in, oavsett om de lyckats eller misslyckats.

    b) Utloggning (även tidsutlöst utloggning i förekommande fall).

    c) Skapande, radering och ändring av åtkomsttyp och åtkomsträttigheter.

    d) Skapande, radering och ändring av lösenord.

22. För alla ovannämnda händelser ska åtminstone följande uppgifter anges:

    a) Händelsetyp.

    b) Användarnamn.

    c) Datum och klockslag.

    d) Enhet.

23. Redovisningsregistren bör hjälpa den säkerhetsansvariga att undersöka potentiella säkerhetsincidenter. De kan också användas som underlag för eventuella rättsliga utredningar av säkerhetsincidenter. Alla säkerhetsregister bör kontrolleras regelbundet för att kartlägga potentiella säkerhetsincidenter. Redovisningsregistren ska skyddas från otillåten radering eller ändring.

24. Bidragsmottagaren ska ha en fastställd hanteringsstrategi för säkerhetsincidenter. Användare och administratörer ska informeras om hur de ska hantera och rapportera incidenter och vad som ska göras i nödsituationer.

25. Om uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED har läckt eller misstänks ha läckt ska detta rapporteras till den bidragsbeviljande myndigheten. Rapporten ska innehålla en beskrivning av de berörda uppgifterna och omständigheterna kring den konstaterade eller misstänkta läckan. Alla användare måste få veta hur de ska rapportera faktiska och misstänkta säkerhetsincidenter till den säkerhetsansvariga.

Nätverk och sammankoppling

26. Om bidragsmottagaren kommunikations- och informationssystem för hantering av uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED är sammankopplat med ett kommunikations- och informationssystem som inte är ackrediterat, ökar detta väsentligt risken både för säkerheten i entreprenörens kommunikations- och informationssystem och för de uppgifter som hanteras i systemet. Detta avser såväl internet som andra offentliga eller privata kommunikations- och informationssystem, även bidragsmottagarnas eller underentreprenörernas övriga system. I så fall ska bidragsmottagaren göra en riskbedömning för att kartlägga de ytterligare säkerhetskrav som bör uppfyllas som ett led i förfarandet för säkerhetsackreditering. Bidragsmottagaren ska förse den bidragsbeviljande myndigheten, och där så krävs enligt nationella lagar och andra föreskrifter även den behöriga ackrediteringsmyndigheten för säkerhet, med ett överensstämmelseintyg som styrker att bidragsmottagarens kommunikations- och informationssystem och därmed sammankopplade system har ackrediterats för hantering av säkerhetsskyddsklassificerade EU-uppgifter på nivån RESTREINT UE/EU RESTRICTED.

27. Fjärråtkomst från andra system till LAN-tjänster (till exempel fjärråtkomst till e-post och systemsupport) är förbjuden om inte särskilda säkerhetsåtgärder vidtagits och godkänts av den bidragsbeviljande myndigheten, och om detta krävs enligt nationella lagar och andra föreskrifter även av den behöriga ackrediteringsmyndigheten för säkerhet.

Konfigurationsstyrning

28. En ingående konfigureringsbeskrivning av maskin- och programvara enligt dokumentationen för ackreditering/godkännande (även diagram över system och nätverk) ska finnas tillhanda och regelbundet uppdateras.

29. Bidragsmottagarens säkerhetsansvariga ska göra konfigurationskontroller av maskin- och programvara för att se till att ingen otillåten maskin- eller programvara förts in.

30. Förändringar i konfigurationen av bidragsmottagarens kommunikations- och informationssystem ska bedömas ur säkerhetssynpunkt och godkännas av den säkerhetsansvariga, och om detta krävs enligt nationella lagar och andra föreskrifter även av ackrediteringsmyndigheten för säkerhet.

31. Säkerhetsbrister i systemet ska sökas minst en gång i kvartalet. Programvara som ska spåra sabotageprogram ska installeras och uppdateras. Om möjligt ska sådan programvara vara föremål för nationellt godkännande eller ett erkänt internationellt godkännande eller följa en allmänt accepterad industristandard.

32. Bidragsmottagaren ska utarbeta en kontinuitetsplan. Rutiner för säkerhetskopiering ska fastställas för följande:

    a) Hur ofta säkerhetskopiering ska göras.

    b) Krav på hur säkerhetskopior ska lagras på plats (brandsäkra behållare) eller på annan plats.

    c) Kontroll av tillåten tillgång till säkerhetskopior.

Fysisk radering och förstöring

33. När kommunikations- och informationssystem och datalagringsmedier någon gång innehållit uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED måste följande fysiska radering göras på hela systemet eller lagringsmediet innan det bortskaffas:

    a) Flashminnen (t.ex. USB-minnen, SD-kort, SSD-minnen eller hybridhårddiskar) måste skrivas över minst tre gånger och därefter kontrolleras för att säkerställa att det ursprungliga innehållet inte kan återskapas; alternativt ska de raderas med hjälp av godkänd programvara.

    b) Magnetiska lagringsmedier (t.ex. hårddiskar) måste skrivas över eller avmagnetiseras.

    c) Optiska medier (t.ex. CD-skivor och DVD) måste strimlas eller sönderdelas.

    d) För övriga typer av lagringsmedier bör den bidragsbeviljande myndigheten eller om det är lämpligt den nationella säkerhetsmyndigheten, utsedda säkerhetsmyndigheten eller ackrediteringsmyndigheten för säkerhet höras om vilka säkerhetskrav som ska uppfyllas.

34. Uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED måste fysiskt raderas på alla typer av datalagringsmedier innan dessa överlämnas till något organ som inte är behörigt att få tillgång till uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED (t.ex. för underhållsarbete).

BILAGA IV

Säkerhetsgodkännande av verksamhetsställe och personal för bidragsmottagare eller underentreprenörer som hanterar uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED samt nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter som kräver anmälan av säkerhetsskyddsklassificerade bidragsavtal som gäller uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED [1]

Medlemsstat	Säkerhetsgodkännande av verksamhetsställe		Anmälan till nationella säkerhetsmyndigheter eller utsedda myndigheter av bidragsavtal eller underentreprenörsavtal som avser säkerhetsnivån R-UE/EU-R		Personalsäkerhetsgodkännande	
	JA	NEJ	JA	NEJ	JA	NEJ
Belgien		**X**		**X**		**X**
Bulgarien		**X**		**X**		**X**
Tjeckien		**X**		**X**		**X**
Danmark	**X**		**X**		**X**	
Tyskland		**X**		**X**		**X**
Estland	**X**		**X**			**X**
Irland		**X**		**X**		**X**
Grekland	**X**			**X**	**X**	
Spanien		**X**	**X**			**X**
Frankrike		**X**		**X**		**X**
Kroatien		**X**	**X**			**X**
Italien		**X**	**X**			**X**
Cypern		**X**	**X**			**X**
Lettland		**X**		**X**		**X**
Litauen	**X**		**X**			**X**
Luxemburg	**X**		**X**		**X**	
Ungern		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Nederländerna	**X** (endast för försvarsrelaterade bidragsavtal och underentreprenörsavtal)		**X** (endast för försvarsrelaterade bidragsavtal och underentreprenörsavtal)			**X**
Österrike		**X**		**X**		**X**
Polen		**X**		**X**		**X**

[1] Dessa nationella krav avseende säkerhetsgodkännande av verksamhetsställe och personalsäkerhetsgodkännande samt anmälan av bidragsavtal som gäller uppgifter som säkerhetsklassats på nivån RESTREINT UE/EU RESTRICTED får inte lägga ytterligare skyldigheter på andra medlemsstater eller bidragsmottagare och underentreprenörer inom deras jurisdiktion.
Anmälan av bidragsavtal som gäller uppgifter som säkerhetsklassats på nivån CONFIDENTIEL UE/EU CONFIDENTIAL eller SECRET UE/EU SECRET är obligatorisk.

Portugal		**X**		**X**		**X**
Rumänien		**X**		**X**		**X**
Slovenien	**X**		**X**			**X**
Slovakien	**X**		**X**			**X**
Finland		**X**		**X**		**X**
Sverige		**X**		**X**		**X**

BILAGA V

FÖRTECKNING ÖVER AVDELNINGAR VID NATIONELLA SÄKERHETSMYNDIGHETER/UTSEDDA SÄKERHETSMYNDIGHETER MED ANSVAR FÖR FÖRFARANDEN AVSEENDE INDUSTRISÄKERHET

BELGIEN

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels

Tfn +32 25014542 (Secretariat)

Fax +32 25014596

E-post: nvo-ans@diplobel.fed.be

BULGARIEN

1. State Commission on Information Security - National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tfn +359 29835775
   Fax +359 29873750
   E-post: dksi@government.bg

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

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

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

(De ovan förtecknade behöriga myndigheterna utför säkerhetsprövning för utfärdande av säkerhetsgodkännande av verksamhetsställe till juridiska personer som vill ingå kontrakt som kräver säkerhetsavtal och personalsäkerhetsgodkännande för enskilda som fullgör kontrakt som kräver säkerhetsavtal för dessa myndigheters räkning.)

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.

   1407 Sofia

   Tfn +359 28147109

   Fax +359 29632188, +359 28147441

   E-post: dans@dans.bg

(De ovanstående säkerhetstjänsterna utför säkerhetsprövning för utfärdande av säkerhetsgodkännande av verksamhetsställe och personalsäkerhetsgodkännande till alla andra juridiska personer och enskilda i landet som vill ingå eller genomför kontrakt eller säkerhetsskyddsklassificerade bidragsavtal som kräver säkerhetsavtal.)

TJECKIEN

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Prag 56

Tfn +420 257283129

E-post: sbr@nbu.cz

DANMARK

1. Politiets Efterretningstjeneste
   (danska säkerhetsunderrättelsetjänsten)

   Klausdalsbrovej 1

   2860 Søborg

   Tfn +45 33148888

   Fax +45 33430190

2. Forsvarets Efterretningstjeneste
   (danska försvarsunderrättelsetjänsten)
   Kastellet 30
   2100 Köpenhamn Ø

   Tfn +45 33325566

   Fax +45 33931320

TYSKLAND

1. För frågor som rör industrisäkerhet, säkerhetsgodkännande av verksamhetsställe och transportplaner (ej kryptomaterial eller konfidentiell affärsinformation):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Tfn +49 228996154028

   Fax +49 228996152676

   E-post: dsagermany-rs3@bmwi.bund.de (e-postadress till kontoret)

2. För sedvanlig begäran om besök till eller från tyska företag:

   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division – RS2
   Villemombler Str. 76
   53123 Bonn

   Tfn +49 228996152401

   Fax +49 228996152603

   E-post: rs2-international@bmwi.bund.de (e-postadress till kontoret)

3. Transportplaner för kryptoprodukter:

   Federal Office for Information Security (BSI)
   National Distribution Agency / NDA-EU DEU
   Mainzer Str. 84
   53179 Bonn

   Tfn +49 2289995826052

   Fax +49 228991095826052

   E-post: NDAEU@bsi.bund.de

ESTLAND

Nationell säkerhetsmyndighetsavdelning
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn

Tfn +372 6939211

Fax +372 6935001

E-post: nsa@fis.gov.ee

IRLAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45

Tfn +353 14082724

E-post: nsa@dfa.ie

GREKLAND

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens

Tfn +30 2106572022, +30 2106572178

Fax +30 2106527612

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

SPANIEN

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

Tfn +34 912832583, +34 912832752, +34 913725928

Fax +34 913725808

E-post: nsa-sp@areatec.com

För information om säkerhetsskyddsklassificerade program: programas.ons@areatec.com

I frågor som gäller personalsäkerhetsgodkännande: hps.ons@areatec.com

I frågor som gäller transportplaner och internationella besök: sp-ivtco@areatec.com

FRANKRIKE

Nationell säkerhetsmyndighet (policy och genomförande på områden som inte rör försvarsindustriella frågor)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tfn +33 171758193

Fax +33 171758200

E-post: ANSFrance@sgdsn.gouv.fr

Utsedd säkerhetsmyndighet (genomförande i försvarsindustriella frågor)
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

Tfn +33 988670421

E-post: För formulär och avsändning av begäran om besök: dga-ssdi.ai.fct@intradef.gouv.fr

För mottagande av begäran om besök: dga-ssdi.visit.fct@intradef.gouv.fr

KROATIEN

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

Tfn +385 14681222

Fax +385 14686049

E-post: NSACroatia@uvns.hr

ITALIEN

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

Tfn +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-post: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia

Tfn +357 22807569, +357 22807764

Fax +357 22302351

E-post: cynsa@mod.gov.cy

LETTLAND

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

Tfn +371 67025418, +371 67025463

Fax +371 67025454

E-post: ndi@sab.gov.lv, ndi@zd.gov.lv

LITAUEN

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Republiken Litauens kommission för samordning av hemlighetsskydd)
Nationell säkerhetsmyndighet
Pilaitės pr. 19
LT-06264 Vilnius

Tfn +370 70666128

E-post: nsa@vsd.lt

LUXEMBURG

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

Tfn +352 24782210

E-post: ans@me.etat.lu

UNGERN

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tfn +36 13911862

Fax +36 13911889

E-post: 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

Tfn +356 23952000

Fax +356 21242406

E-post: certification@mccaa.org.mt

NEDERLÄNDERNA

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA Haag

   Tfn +31 703204400

   Fax +31 703200733

   E-post: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES Haag

   Tfn +31 704419407

   Fax +31 703459189

   E-post: indussec@mindef.nl

ÖSTERRIKE

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tfn +43 153115202594

   E-post: isk@bka.gv.at

2. Utsedd säkerhetsmyndighet på militärområdet:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   E-post: abwa@bmlvs.gv.at

POLEN

Intern säkerhetsmyndighet
Avdelningen för skydd av säkerhetsskyddsklassificerad information
Rakowiecka 2A
00-993 Warszawa

Tfn +48 225857944

Fax +48 225857443

E-post: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lissabon

Tfn +351 213031710

Fax +351 213031711

E-post: sind@gns.gov.pt, franco@gns.gov.pt

RUMÄNIEN

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Rumäniens nationella säkerhetsmyndighet - ORNISS - nationell registreringsmyndighet för säkerhetsskyddsklassificerad information
4th Mures Street
012275 Bukarest

Tfn +40 212075115

Fax +40 212245830

E-post: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIEN

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SI-1000 Ljubljana

Tfn +386 14781390

Fax: +386 14781399

E-post: gp.uvtp@gov.si

SLOVAKIEN

Národný bezpečnostný úrad
(nationella säkerhetsmyndigheten)
Avdelningen för säkerhetsgodkännande
Budatínska 30 P.O.
851 06 Bratislava Slovakien

Tfn +421 268691111

Fax +421 268691700

E-post: podatelna@nbu.gov.sk

FINLAND

Nationell säkerhetsmyndighet
Utrikesministeriet
P.O. Box 453
FI-00023 Statsrådet

E-post: NSA@formin.fi

SVERIGE

1. Nationell säkerhetsmyndighet
   Utrikesdepartementet
   UD SÄK / NSA
   SE-103 39 Stockholm
   Tfn +46 84051000
   Fax +46 87231176
   E-post: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tfn +46 87824000
   Fax +46 87826900
   E-post: security@fmv.se