DECISIONE (UE, Euratom) 2021/259 DELLA COMMISSIONE

del 10 febbraio 2021

che stabilisce le norme di attuazione in materia di sicurezza industriale per quanto riguarda le sovvenzioni classificate

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 249,

visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 106,

visto il regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 ([1]),

vista la decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione ([2]),

vista la decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE ([3]),

vista la decisione (UE, Euratom) 2017/46 della Commissione, del 10 gennaio 2017, sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea ([4]),

previa consultazione del gruppo di esperti in materia di sicurezza della Commissione a norma dell'articolo 41, paragrafo 5, della decisione (UE, Euratom) 2015/444,

considerando quanto segue:

(1) Gli articoli 41, 42, 47 e 48 della decisione (UE, Euratom) 2015/444 della Commissione prevedono che siano stabilite disposizioni più dettagliate a integrazione e supporto del capo 6 della medesima decisione mediante norme di attuazione in materia di sicurezza industriale per disciplinare aspetti quali l'aggiudicazione di convenzioni di sovvenzione classificate, il nulla osta di sicurezza delle imprese, il nulla osta di sicurezza del personale, le visite e la trasmissione e il trasporto delle informazioni classificate UE (ICUE).

(2) La decisione (UE, Euratom) 2015/444 stabilisce che l'attuazione delle convenzioni di sovvenzione classificate avvenga in stretta collaborazione con l'autorità di sicurezza nazionale, l'autorità di sicurezza designata o altra autorità competente degli Stati membri interessati. Gli Stati membri hanno convenuto di provvedere affinché qualsiasi soggetto sotto la loro giurisdizione che può ottenere o produrre informazioni classificate provenienti dalla Commissione sia in possesso di un nulla osta di sicurezza adeguato e sia in grado di assicurare la protezione di sicurezza del livello adeguato, equivalente a quella accordata dalle norme di sicurezza del Consiglio dell'Unione europea per proteggere le informazioni classificate UE che recano un contrassegno di classifica corrispondente, secondo quanto previsto dall'accordo tra gli Stati membri dell'Unione europea, riuniti in sede di Consiglio, sulla protezione delle informazioni classificate scambiate nell'interesse dell'Unione europea (2011/C 202/05) ([5]).

([1]) GU L 193 del 30.7.2018, pag. 1.
([2]) GU L 72 del 17.3.2015, pag. 41.
([3]) GU L 72 del 17.3.2015, pag. 53.
([4]) GU L 6 dell'11.1.2017, pag. 40.
([5]) GU C 202 dell'8.7.2011, pag. 13.

(3) Il Consiglio, la Commissione e l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno convenuto di garantire la massima coerenza nell'applicazione delle norme di sicurezza relative alla protezione delle ICUE tenendo conto allo stesso tempo delle loro specifiche esigenze istituzionali e organizzative, conformemente alle dichiarazioni allegate al verbale della sessione del Consiglio in cui è stata adottata la decisione 2013/488/UE del Consiglio ([6]) sulle norme di sicurezza per proteggere le informazioni classificate UE.

(4) Le norme di attuazione della Commissione in materia di sicurezza industriale per quanto riguarda le sovvenzioni classificate dovrebbero pertanto garantire anche la massima coerenza e tenere conto degli orientamenti sulla sicurezza industriale approvati dal comitato per la sicurezza del Consiglio il 13 dicembre 2016.

(5) Il 4 maggio 2016 la Commissione ha adottato una decisione ([7]) che abilita il membro della Commissione responsabile per le questioni di sicurezza ad adottare, a nome della Commissione e sotto la sua responsabilità, le norme di attuazione a norma dell'articolo 60 della decisione (UE, Euratom) 2015/444,

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. La presente decisione stabilisce le norme di attuazione in materia di sicurezza industriale per quanto riguarda le sovvenzioni classificate ai sensi della decisione (UE, Euratom) 2015/444, in particolare il capo 6 della medesima.

2. La presente decisione stabilisce requisiti specifici per garantire la protezione delle informazioni classificate UE (ICUE) durante la pubblicazione degli inviti, l'aggiudicazione di sovvenzioni e l'attuazione delle convenzioni di sovvenzione classificate concluse dalla Commissione europea.

3. La presente decisione si applica alle sovvenzioni comportanti informazioni classificate del livello seguente:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

4. La presente decisione si applica fatte salve le norme specifiche stabilite in altri atti giuridici, come quelle riguardanti il programma europeo di sviluppo del settore industriale della difesa.

Articolo 2

Responsabilità in seno alla Commissione

1. Nell'ambito delle sue responsabilità l'ordinatore dell'autorità erogatrice, di cui al regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, garantisce che la sovvenzione classificata è conforme alla decisione (UE, Euratom) 2015/444 e alle relative norme di attuazione.

([6]) Decisione del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).

([7]) Decisione della Commissione, del 4 maggio 2016, relativa alla delega di poteri in materia di sicurezza [C(2016) 2797 final].

2. A tal fine in tutte le fasi l'ordinatore interessato chiede il parere dell'autorità di sicurezza della Commissione sulle questioni riguardanti gli elementi di sicurezza della convenzione di sovvenzione classificata, del programma o del progetto classificato e informa il responsabile locale della sicurezza in merito alle convenzioni di sovvenzione classificate firmate. La decisione sul livello di classifica di determinate materie spetta all'autorità erogatrice ed è presa tenendo in debito conto la guida alle classifiche di sicurezza.

3. Se si applicano le istruzioni di sicurezza del programma/progetto di cui all'articolo 5, paragrafo 3, l'autorità erogatrice e l'autorità di sicurezza della Commissione assolvono le responsabilità loro assegnate in tali istruzioni.

4. Nel rispetto dei requisiti delle presenti norme di attuazione, l'autorità di sicurezza della Commissione collabora strettamente con le autorità di sicurezza nazionali (NSA) e le autorità di sicurezza designate (DSA) degli Stati membri interessati, in particolare per quanto riguarda il nulla osta di sicurezza delle imprese (FSC) e il nulla osta di sicurezza del personale (PSC), la procedura relativa alle visite e i programmi di trasporto.

5. Se le sovvenzioni sono gestite da agenzie esecutive dell'UE o da altri organismi di finanziamento e non si applicano le norme specifiche stabilite in altri atti giuridici di cui all'articolo 1, paragrafo 4:

(a) il servizio della Commissione delegante esercita i diritti dell'originatore di ICUE generate nel contesto delle sovvenzioni, se previsto dalle modalità di delega;

(b) il servizio della Commissione delegante ha la responsabilità di stabilire la classifica di sicurezza;

(c) le richieste di informazioni sui nulla osta di sicurezza e le comunicazioni alle NSA e/o alle DSA sono trasmesse tramite l'autorità di sicurezza della Commissione.

CAPO 2

GESTIONE DEGLI INVITI PER SOVVENZIONI CLASSIFICATE

Articolo 3

Principi di base

1. Le parti classificate delle sovvenzioni sono attuate esclusivamente da beneficiari registrati in uno Stato membro o da beneficiari registrati in un paese terzo o istituiti da un'organizzazione internazionale, purché il paese terzo o l'organizzazione internazionale abbia concluso un accordo sulla sicurezza delle informazioni con l'Unione o un accordo amministrativo con la Commissione ([8]).

2. Prima di pubblicare l'invito per una sovvenzione classificata, l'autorità erogatrice determina la classifica di sicurezza delle informazioni a cui potrebbero avere accesso i richiedenti. L'autorità erogatrice determina anche la classifica di sicurezza massima delle informazioni generate durante l'esecuzione della convenzione di sovvenzione, del programma o del progetto, o almeno il volume e il tipo delle informazioni che si prevede di produrre o trattare e stabilisce la necessità di un sistema di comunicazione e informazione (CIS) classificato.

3. L'autorità erogatrice provvede affinché gli inviti per sovvenzioni classificate diano informazioni sugli obblighi specifici di sicurezza connessi a dette informazioni. La documentazione dell'invito comprende chiarimenti sulle tempistiche a disposizione dei beneficiari per ottenere gli FSC ove necessario. Gli allegati I e II contengono modelli delle informazioni relative alle condizioni dell'invito.

([8]) Sul sito web della Commissione è disponibile l'elenco degli accordi conclusi dall'UE e degli accordi amministrativi conclusi dalla Commissione europea, in base ai quali possono essere scambiate informazioni classificate UE con i paesi terzi e le organizzazioni internazionali.

4. L'autorità erogatrice provvede affinché le informazioni classificate RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET siano comunicate ai richiedenti solo dopo che questi ultimi abbiano firmato l'impegno alla non divulgazione, che li obbliga a trattare e proteggere le ICUE a norma della decisione (UE, Euratom) 2015/444, e relative norme di attuazione e delle norme nazionali applicabili.

5. Quando ai richiedenti sono comunicate informazioni RESTREINT UE/EU RESTRICTED, nell'invito o negli accordi di non divulgazione conclusi nella fase di proposta sono inseriti i requisiti minimi di cui all'articolo 5, paragrafo 7, della presente decisione.

6. Tutti i richiedenti e i beneficiari tenuti a trattare o conservare informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nelle loro strutture nella fase di proposta o durante l'esecuzione della convenzione di sovvenzione classificata sono in possesso dell'FSC del livello richiesto, ad eccezione dei casi di cui al paragrafo 9. Di seguito sono indicate le tre situazioni che possono presentarsi nella fase di proposta relativa a una sovvenzione classificata che comporta ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET:

(a) nessun accesso alle ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nella fase di proposta:

se l'invito riguarda una sovvenzione che comporterà ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, ma il richiedente non sarà tenuto a trattare dette informazioni nella fase di proposta, il mancato possesso da parte del richiedente dell'FSC del livello richiesto non determina l'esclusione dalla procedura di presentazione della domanda;

(b) accesso alle ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei locali dell'autorità erogatrice nella fase di proposta:

l'accesso è consentito al personale del richiedente che sia in possesso del PSC del livello richiesto e che abbia necessità di conoscere;

(c) trattamento o conservazione delle ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei locali del richiedente nella fase di proposta:

se l'invito impone ai richiedenti di trattare o conservare le ICUE nei loro locali, il richiedente deve essere in possesso dell'FSC del livello richiesto. In questi casi l'autorità erogatrice ottiene, tramite l'autorità di sicurezza della Commissione, l'assicurazione dell'NSA o della DSA competente che al richiedente è stato rilasciato l'FSC adeguato prima che gli sia consegnato il materiale delle ICUE. L'accesso è consentito al personale del richiedente che sia in possesso del PSC del livello richiesto e che abbia necessità di conoscere.

7. Di norma non è richiesto l'FSC o il PSC per l'accesso alle informazioni RESTREINT UE/EU RESTRICTED, né nella fase di proposta né in quella di esecuzione della convenzione di sovvenzione. Quando gli Stati membri prescrivono l'FSC o il PSC per convenzioni di sovvenzione o subcontratti di livello RESTREINT UE/EU RESTRICTED a norma di disposizioni legislative e regolamentari nazionali, come indicato nell'allegato IV, le prescrizioni nazionali non possono imporre obblighi supplementari agli altri Stati membri né impedire ai richiedenti, beneficiari o subcontraenti di Stati membri che non prevedono dette prescrizioni in materia di FSC o PSC l'accesso a informazioni RESTREINT UE/EU RESTRICTED derivanti da convenzioni di sovvenzione o da subcontratti connessi o la partecipazione alla relativa gara. Queste convenzioni di sovvenzione sono eseguite negli Stati membri conformemente alle rispettive disposizioni legislative e regolamentari nazionali.

8. Quando nella gestione di un invito è richiesto l'FSC per l'attuazione di una convenzione di sovvenzione classificata, l'autorità erogatrice ne fa richiesta, tramite l'autorità di sicurezza della Commissione, all'NSA o alla DSA del beneficiario utilizzando il modulo di informazione sul nulla osta di sicurezza delle imprese (FSCIS) o altro modello elettronico equivalente previsto. L'allegato III, appendice D, riporta un modello di FSCIS ([9]). Se possibile, la risposta all'FSCIS è data entro dieci giorni lavorativi dalla data della richiesta.

9. Se istituzioni pubbliche degli Stati membri o istituti soggetti al controllo del loro governo partecipano a sovvenzioni classificate per cui sono necessari FSC e se il diritto nazionale non prevede il rilascio di FSC a tali istituzioni e istituti, l'autorità erogatrice verifica con la NSA o la DSA interessata, tramite l'autorità di sicurezza della Commissione, se dette istituzioni o istituti sono in grado di trattare le ICUE al livello richiesto.

([9]) Altri modelli utilizzati possono presentare differenze di forma rispetto al modello fornito nelle presenti norme di attuazione.

10. Se per l'esecuzione di una convenzione di sovvenzione classificata è necessario un PSC e se a norma delle disposizioni nazionali occorre un FSC perché sia rilasciato un PSC, l'autorità erogatrice verifica con l'NSA o la DSA del beneficiario, tramite l'autorità di sicurezza della Commissione utilizzando un FSCIS, se il beneficiario è in possesso di un FSC o se è in corso il processo per ottenere l'FSC. In questo caso la Commissione non fa richiesta di PSC utilizzando il modulo di informazione sul nulla osta di sicurezza del personale («PSCIS»).

Articolo 4

Subcontratti delle sovvenzioni classificate

1. Le condizioni alle quali i beneficiari possono subappaltare azioni relative alle prestazioni che comportano ICUE sono definite nell'invito e nella convenzione di sovvenzione. Tali condizioni comprendono l'obbligo che tutti i FSCIS siano trasmessi tramite l'autorità di sicurezza della Commissione. Il subcontratto è subordinato al previo consenso scritto dell'autorità erogatrice. Se del caso, il subcontratto deve essere conforme all'atto di base che istituisce il programma.

2. Le parti classificate delle sovvenzioni sono subappaltate esclusivamente a soggetti registrati in uno Stato membro o a soggetti registrati in un paese terzo o istituiti da un'organizzazione internazionale, purché il paese terzo o l'organizzazione internazionale abbiano concluso un accordo sulla sicurezza delle informazioni con l'Unione o un accordo amministrativo con la Commissione ([10]).

CAPO 3

GESTIONE DI SOVVENZIONI CLASSIFICATE

Articolo 5

Principi di base

1. In sede di aggiudicazione di una sovvenzione classificata, l'autorità erogatrice, assieme all'autorità di sicurezza della Commissione, garantisce che gli obblighi dei beneficiari in materia di protezione delle ICUE usate o generate nel corso dell'esecuzione della convenzione di sovvenzione siano parte integrante della convenzione. I requisiti di sicurezza specifici della sovvenzione assumono la forma di una lettera sugli aspetti di sicurezza (SAL). Nell'allegato III è riportato un modello di SAL.

2. Prima della firma della sovvenzione classificata, l'autorità erogatrice approva una guida alle classifiche di sicurezza (SCG) in cui sono descritti i compiti da svolgere e le informazioni generate nell'attuazione della sovvenzione, o se del caso a livello di programma o di progetto. La SCG è inclusa nella SAL.

3. I requisiti di sicurezza specifici del programma o del progetto assumono la forma di istruzioni di sicurezza del programma/progetto (PSI). Le PSI possono essere redatte sulla base delle disposizioni del modello di SAL di cui all'allegato III. Sono elaborate dal servizio della Commissione responsabile della gestione del programma o del progetto, in stretta collaborazione con l'autorità di sicurezza della Commissione, e presentate per parere al gruppo di esperti in materia di sicurezza della Commissione. Se una convenzione di sovvenzione rientra in un programma o in un progetto dotato delle proprie PSI, la SAL della convenzione è redatta in forma semplificata e rinvia alle disposizioni in materia di sicurezza contenute nelle PSI del programma/progetto.

4. Ad eccezione dei casi di cui all'articolo 3, paragrafo 9, la convenzione di sovvenzione classificata non è firmata fino a quando l'NSA o la DSA del richiedente non ne abbia confermato l'FSC o, se è un consorzio ad aggiudicarsi la convenzione di sovvenzione classificata, fino a quando l'NSA o la DSA di almeno un richiedente all'interno del consorzio, o più se necessario, non abbia confermato l'FSC di tale richiedente.

5. In linea di principio e salvo diversamente disposto da altre norme pertinenti l'autorità erogatrice è considerata l'originatore di ICUE generate nell'esecuzione della convenzione di sovvenzione.

([10]) Sul sito web della Commissione è disponibile l'elenco degli accordi conclusi dall'UE e degli accordi amministrativi conclusi dalla Commissione europea, in base ai quali possono essere scambiate informazioni classificate UE con i paesi terzi e le organizzazioni internazionali.

6. L'autorità erogatrice, tramite l'autorità di sicurezza della Commissione, notifica alle NSA e o alle DSA di tutti i beneficiari e subcontraenti la firma di convenzioni di sovvenzione o subcontratti classificati e la loro eventuale proroga o estinzione anticipata. Nell'allegato IV è riportato l'elenco delle prescrizioni per paese.

7. Le convenzioni di sovvenzione che comportano informazioni classificate RESTREINT UE/EU RESTRICTED includono una clausola di sicurezza che rende vincolanti per i beneficiari le disposizioni di cui all'allegato III, appendice E. Tali convenzioni di sovvenzione includono la SAL che stabilisce come minimo i requisiti per il trattamento delle informazioni RESTREINT UE/EU RESTRICTED, compresi gli aspetti relativi alla garanzia di sicurezza delle informazioni e i requisiti specifici che devono rispettare i beneficiari per l'accreditamento del loro CIS che tratta informazioni RESTREINT UE/EU RESTRICTED.

8. Ove previsto dalle disposizioni legislative e regolamentari degli Stati membri, le NSA o le DSA garantiscono che i beneficiari o i subcontraenti sotto la loro giurisdizione rispettino le disposizioni di sicurezza applicabili per la protezione delle informazioni RESTREINT UE/EU RESTRICTED e svolgono visite di verifica presso le strutture dei beneficiari o dei subcontraenti situate sul loro territorio. Se l'NSA o la DSA non è soggetta a tale obbligo, l'autorità erogatrice garantisce che i beneficiari attuino le disposizioni di sicurezza richieste di cui all'allegato III, appendice E.

Articolo 6

Accesso alle ICUE del personale dei beneficiari e dei subcontraenti

1. L'autorità erogatrice assicura che le convenzioni di sovvenzione classificate contengano disposizioni secondo le quali il personale dei beneficiari o dei subcontraenti che per l'esecuzione della convenzione di sovvenzione classificata o del subcontratto debba avere accesso alle ICUE può ottenere tale accesso soltanto se:

(a) è stato stabilito che ha necessità di conoscere;

(b) per le informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, l'NSA o la DSA o altra autorità di sicurezza competente gli ha rilasciato il nulla osta di sicurezza di livello appropriato;

(c) è stato istruito sulle norme di sicurezza applicabili per la protezione delle ICUE e ha riconosciuto le proprie responsabilità in materia di protezione di tali informazioni.

2. Se del caso, l'accesso alle ICUE deve altresì essere conforme all'atto di base che stabilisce il programma e tiene conto di eventuali contrassegni supplementari definiti nell'SCG.

3. Se il beneficiario o il subcontraente intende assumere un cittadino di un paese non UE in una posizione che richiede l'accesso a ICUE classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, spetta a detto beneficiario o subcontraente avviare la procedura per il rilascio del nulla osta di sicurezza per tale cittadino a norma delle disposizioni legislative e regolamentari nazionali applicabili nel luogo in cui deve essere concesso l'accesso alle ICUE.

Articolo 7

Accesso alle ICUE da parte degli esperti che partecipano a controlli, esami o audit

1. Le persone esterne («esperti») che partecipano ai controlli, agli esami o audit effettuati dall'autorità erogatrice o alle valutazioni dei risultati dei beneficiari per cui è necessario accedere a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, ricevono un contratto solo se hanno ottenuto il nulla osta di sicurezza al livello appropriato dalla rispettiva NSA o DSA o da altra autorità di sicurezza competente. L'autorità erogatrice, tramite l'autorità di sicurezza della Commissione, verifica e se del caso chiede all'NSA o alla DSA di avviare accertamenti sugli esperti almeno sei mesi prima dell'inizio dei rispettivi contratti.

2. Prima di firmare il contratto, gli esperti sono istruiti sulle norme di sicurezza applicabili per la protezione delle ICUE e riconoscono le proprie responsabilità in materia di protezione delle stesse.

CAPO 4

VISITE IN RELAZIONE A CONVENZIONI DI SOVVENZIONE CLASSIFICATE

Articolo 8

Principi di base

1. Se l'autorità erogatrice, gli esperti, i beneficiari o i subcontraenti richiedono l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei reciproci locali per l'esecuzione della convenzione di sovvenzione classificata, le visite sono organizzate di concerto con le NSA o DSA o altra autorità di sicurezza competente interessata.

2. Le visite di cui al paragrafo 1 sono soggette alle condizioni seguenti:

(a) la visita deve avere uno scopo ufficiale inerente a una sovvenzione classificata;

(b) per accedere alle ICUE utilizzate o generate nell'esecuzione di una sovvenzione classificata i visitatori devono essere in possesso del PSC al livello richiesto e avere la necessità di conoscere.

Articolo 9

Richiesta di visita

1. Le visite dei beneficiari o dei subcontraenti presso le strutture di altri beneficiari o subcontraenti o presso i locali dell'autorità erogatrice che comportano l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono organizzate secondo la procedura seguente:

(a) il responsabile della sicurezza della struttura che invia il visitatore deve compilare tutte le parti pertinenti del modulo per la richiesta di visita (RFV) e presentare la richiesta all'NSA o alla DSA della struttura. Nell'allegato III, appendice C, è riportato un modello del modulo RFV;

(b) l'NSA o la DSA della struttura che invia il visitatore deve confermare il PSC del visitatore prima di inoltrare l'RFV all'NSA o alla DSA della struttura ospitante (o all'autorità di sicurezza della Commissione se la visita avviene nei locali dell'autorità erogatrice);

(c) il responsabile della sicurezza della struttura che invia il visitatore deve poi acquisire dalla propria NSA o DSA la risposta dell'NSA o della DSA della struttura ospitante (o dell'autorità di sicurezza della Commissione) di approvazione o di rigetto dell'RFV;

(d) l'RFV è considerata approvata se non vengono sollevate obiezioni fino ai cinque giorni lavorativi precedenti la data della visita.

2. Le visite di funzionari dell'autorità erogatrice o di esperti o revisori presso le strutture dei beneficiari o dei subcontraenti che comportano l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono organizzate secondo la procedura seguente:

(a) il visitatore deve compilare tutte le parti pertinenti del modulo RFV e inoltrarlo all'autorità di sicurezza della Commissione;

(b) l'autorità di sicurezza della Commissione conferma il PSC del visitatore prima di presentare l'RFV all'NSA o alla DSA della struttura ospitante;

(c) l'autorità di sicurezza della Commissione acquisisce dall'NSA o dalla DSA della struttura ospitante la risposta di approvazione o di rigetto dell'RFV;

(d) l'RFV è considerata approvata se non vengono sollevate obiezioni fino ai cinque giorni lavorativi precedenti la data della visita.

3. L'RFV può riguardare una singola visita o visite ricorrenti. In caso di visite ricorrenti l'RFV può essere valida per un periodo massimo di un anno a decorrere dalla data di inizio richiesta.

4. La durata di validità dell'RFV non può superare la durata di validità del PSC del visitatore.

5. Di norma l'RFV deve essere presentata all'autorità di sicurezza competente della struttura ospitante almeno 15 giorni lavorativi prima della data della visita.

Articolo 10

Procedure di visita

1. Prima di consentire ai visitatori di accedere alle ICUE, l'ufficio di sicurezza della struttura ospitante deve espletare tutte le procedure e rispettare tutte le norme in materia di sicurezza delle visite stabilite dalla propria NSA o DSA.

2. I visitatori devono dimostrare la propria identità all'arrivo presso la struttura ospitante presentando una carta d'identità o un passaporto validi. I dati identificativi devono corrispondere alle informazioni fornite nell'RFV.

3. La struttura ospitante provvede alla tenuta dei registri di tutti i visitatori, contenenti nome e cognome, organizzazione che rappresentano, data di scadenza del PSC, data della visita e nome e cognome delle persone visitate. I registri sono conservati per un periodo di almeno cinque anni, o per un periodo di durata superiore se previsto dalle norme e dai regolamenti nazionali del paese in cui è situata la struttura ospitante.

Articolo 11

Visite organizzate direttamente

1. Nel quadro di progetti specifici le pertinenti NSA o DSA e l'autorità di sicurezza della Commissione possono concordare una procedura in base alla quale le visite per una determinata sovvenzione classificata possono essere organizzate direttamente tra il responsabile della sicurezza del visitatore e il responsabile della sicurezza della struttura da visitare. Il modello di modulo da utilizzare a tal fine figura nell'allegato III, appendice C. Questa procedura eccezionale è definita nelle PSI o in altri accordi specifici. In questi casi non si applicano le procedure di cui all'articolo 9 e all'articolo 10, paragrafo 1.

2. Le visite che comportano l'accesso a informazioni classificate RESTREINT UE/EU RESTRICTED sono organizzate direttamente tra il soggetto che invia e il soggetto che riceve i visitatori senza dover seguire le procedure di cui all'articolo 9 e all'articolo 10, paragrafo 1.

CAPO 5

TRASMISSIONE E TRASPORTO DI ICUE NEL QUADRO DELL'ESECUZIONE DELLE CONVENZIONI DI SOVVENZIONE CLASSIFICATE

Articolo 12

Principi di base

L'autorità erogatrice garantisce che tutte le decisioni relative al trasferimento e al trasporto di ICUE siano conformi alla decisione (UE, Euratom) 2015/444, alle relative norme di attuazione e alle condizioni della convenzione di sovvenzione classificata, compreso il consenso dell'originatore.

Articolo 13

Trattamento elettronico

1. Il trattamento e la trasmissione elettronici delle ICUE sono effettuati conformemente ai capi 5 e 6 della decisione (UE, Euratom) 2015/444 e alle relative norme di attuazione.

I sistemi di comunicazione e informazione di proprietà del beneficiario utilizzati per trattare le ICUE per l'esecuzione della convenzione di sovvenzione (CIS del beneficiario) sono soggetti all'accreditamento da parte dell'autorità di accreditamento di sicurezza (SAA) responsabile. Ogni trasmissione elettronica di ICUE è protetta mediante prodotti crittografici approvati conformemente all'articolo 36, paragrafo 4, della decisione (UE, Euratom) 2015/444. Le misure di sicurezza TEMPEST sono attuate conformemente all'articolo 36, paragrafo 6, della medesima decisione.

2. L'accreditamento di sicurezza del CIS del beneficiario che tratta ICUE di livello RESTREINT UE/EU RESTRICTED e di tutte le relative interconnessioni può essere delegato al responsabile della sicurezza del beneficiario se consentito dalle disposizioni legislative e regolamentari nazionali. In caso di delega il beneficiario è responsabile dell'attuazione dei requisiti minimi di sicurezza descritti nella SAL per il trattamento di informazioni RESTREINT UE/EU RESTRICTED nel suo CIS. Tuttavia le NSA/DSA e le SAA competenti restano responsabili della protezione delle informazioni RESTREINT UE/EU RESTRICTED trattate dal beneficiario e conservano il diritto di ispezionare le misure di sicurezza adottate dal beneficiario. Inoltre il beneficiario trasmette all'autorità erogatrice e se richiesto dalle disposizioni legislative e regolamentari nazionali alla SAA nazionale competente, una dichiarazione di conformità in cui si certifica che il CIS del beneficiario e le relative interconnessioni sono stati accreditati per il trattamento di ICUE di livello RESTREINT UE/EU RESTRICTED ([11]).

Articolo 14

Trasporto mediante corrieri commerciali

Al trasporto di ICUE mediante corrieri commerciali si applicano le pertinenti disposizioni della decisione (UE, Euratom) 2019/1962 della Commissione ([12]) sulle norme di attuazione per il trattamento di informazioni RESTREINT UE/EU RESTRICTED e della decisione (UE, Euratom) 2019/1961 della Commissione ([13]) sulle norme di attuazione per il trattamento di informazioni CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET.

Articolo 15

Trasporto a mano

1. Il trasporto a mano di informazioni classificate è soggetto a rigorosi requisiti di sicurezza.

2. All'interno dell'UE le informazioni RESTREINT UE/EU RESTRICTED possono essere trasportate a mano dal personale del beneficiario, purché siano rispettate le condizioni seguenti:

(a) la busta o l'imballaggio utilizzati devono essere opachi e non recare alcuna indicazione della classificazione del contenuto;

(b) il latore deve portare sempre con sé le informazioni classificate;

(c) la busta o l'imballaggio non devono essere aperti durante il trasporto.

3. Per le informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET il trasporto a mano effettuato dal personale del beneficiario all'interno di uno Stato membro è precedentemente organizzato tra soggetto mittente e soggetto ricevente. L'autorità o la struttura mittente comunica all'autorità o alla struttura ricevente i dettagli della spedizione, compresi il riferimento, la classifica, l'orario previsto di arrivo e il nome del corriere. Il trasporto a mano è consentito, purché siano soddisfatte le condizioni seguenti:

(a) le informazioni classificate devono essere trasportate in doppia busta o doppio imballaggio;

(b) la busta o l'imballaggio esterni devono essere protetti e non devono recare indicazioni della classificazione del contenuto, mentre la busta interna deve recare il livello di classifica;

(c) il latore deve portare sempre con sé le ICUE;

(d) la busta o l'imballaggio non devono essere aperti durante il trasporto;

(e) la busta o l'imballaggio devono essere trasportati in una valigetta chiudibile a chiave o in un contenitore analogo approvato di dimensioni e peso tali da consentire al latore di portarla sempre con sé senza doverla consegnare come bagaglio al seguito;

(f) il corriere deve essere in possesso di un certificato di corriere rilasciato dalla competente autorità di sicurezza che lo autorizza a trasportare la spedizione classificata indicata.

([11]) I requisiti minimi per i sistemi di comunicazione e informazione che trattano ICUE a livello RESTREINT UE/EU RESTRICTED sono stabiliti nell'allegato III, appendice E.

([12]) Decisione (UE, Euratom) 2019/1962 della Commissione, del 17 ottobre 2019, sulle norme di attuazione per il trattamento di informazioni RESTREINT UE/EU RESTRICTED (GU L 311 del 2.12.2019, pag. 21).

([13]) Decisione (UE, Euratom) 2019/1961 della Commissione, del 17 ottobre 2019, sulle norme di attuazione per il trattamento di informazioni CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET (GU L 311 del 2.12.2019, pag. 1).

4. Per il trasporto a mano effettuato dal personale del beneficiario di informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET da uno Stato membro ad un altro si applicano le disposizioni aggiuntive seguenti:

(a) il corriere è responsabile della custodia in condizioni di sicurezza del materiale classificato che trasporta, fino alla consegna al destinatario;

(b) in caso di violazione della sicurezza, l'NSA o la DSA del mittente può chiedere che le autorità del paese in cui si è verificata la violazione effettuino un'indagine, ne riferiscano l'esito e avviino, se del caso, azioni legali o di altro tipo;

(c) il corriere deve essere stato istruito su tutti gli obblighi in materia di sicurezza da rispettare durante il trasporto e deve aver firmato un apposito impegno;

(d) le istruzioni per il corriere sono allegate al certificato di corriere;

(e) il corriere ha ricevuto la descrizione della spedizione e dell'itinerario;

(f) i documenti sono restituiti all'NSA o alla DSA che li ha emessi al termine del viaggio/dei viaggi o sono tenuti a disposizione dal destinatario a fini di controllo;

(g) le autorità doganali, le autorità competenti in materia di immigrazione o la polizia di frontiera che chiedono di esaminare e ispezionare la spedizione sono autorizzate ad aprire e prendere visione di una parte sufficiente che consenta loro di accertare che non contenga materiale diverso da quello dichiarato;

(h) le autorità doganali devono essere sollecitate a rispettare l'autorità ufficiale dei documenti di spedizione e dei documenti di autorizzazione trasportati dal corriere.

L'eventuale apertura della spedizione da parte delle autorità doganali deve avvenire lontano dagli sguardi di persone non autorizzate e, se possibile, in presenza del corriere. Il corriere esige che la spedizione sia reimballata e chiede alle autorità che effettuano l'ispezione di sigillarla nuovamente e di confermare per iscritto che è stata da esse aperta.

5. Il trasporto a mano effettuato dal personale del beneficiario di informazioni classificate RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET verso un paese terzo o un'organizzazione internazionale è soggetto alle disposizioni dell'accordo sulla sicurezza delle informazioni o dell'accordo amministrativo concluso tra, rispettivamente, l'Unione europea o la Commissione e il paese terzo o l'organizzazione internazionale in questione.

CAPO 6

PIANI DI CONTINUITÀ OPERATIVA

Articolo 16

Piani di emergenza e misure di recupero

L'autorità erogatrice garantisce che la convenzione di sovvenzione classificata imponga ai beneficiari di predisporre piani di emergenza (BCP) per proteggere le ICUE trattate nel quadro della sovvenzione classificata in situazioni di emergenza, e di mettere in atto misure di prevenzione e recupero nel contesto di piani di continuità operativa per ridurre al minimo l'impatto degli incidenti in relazione al trattamento e alla conservazione delle ICUE. I beneficiari confermano all'autorità erogatrice l'attuazione dei loro BCP.

Articolo 17

Entrata in vigore

La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 10 febbraio 2021

Per la Commissione
A nome della presidente
Johannes HAHN
Membro della Commissione

ALLEGATO I

INFORMAZIONI STANDARD DA INCLUDERE NEGLI INVITI

(da adattare all'invito utilizzato)

Sicurezza

I progetti che comportano informazioni classificate UE devono essere sottoposti a controllo di sicurezza perché ne sia autorizzato il finanziamento e possono essere soggetti a specifiche norme di sicurezza (precisate nella lettera sugli aspetti di sicurezza (SAL) allegata alla convenzione di sovvenzione).

Tali norme [disciplinate dalla decisione (UE, Euratom) 2015/444 della Commissione ([1]) e/o da norme nazionali] dispongono ad esempio che:

— **NON** possano essere finanziati i progetti che comportano informazioni classificate TRES SECRET UE/EU TOP SECRET (o equivalenti);

— le informazioni classificate debbano essere contrassegnate conformemente alle istruzioni di sicurezza applicabili presenti nella SAL;

— le informazioni con livelli di classifica CONFIDENTIEL UE/EU CONFIDENTIAL o superiori (e RESTREINT UE/EU RESTRICTED se richiesto dalle norme nazionali) possano essere:

  — create o accessibili solo in locali con nulla osta di sicurezza delle imprese rilasciato dalla competente autorità di sicurezza nazionale (NSA) conformemente alle norme nazionali;

  — trattate solo in una zona protetta approvata dall'NSA competente;

  — accessibili e trattate solo da persone che siano in possesso di nulla osta di sicurezza del personale (PSC) valido e che abbiano la necessità di conoscere;

— al termine della sovvenzione le informazioni classificate debbano essere restituite o continuare a essere protette conformemente alle norme applicabili;

— le azioni che comportano informazioni classificate UE (ICUE) possano essere subappaltate solo previa autorizzazione scritta dell'autorità erogatrice e solo a soggetti stabiliti in uno Stato membro dell'UE o in un paese non UE che abbia concluso un accordo sulla sicurezza delle informazioni con l'UE (o un accordo amministrativo con la Commissione);

— la divulgazione di ICUE a terzi sia soggetta alla previa approvazione scritta dell'autorità erogatrice.

Si osservi che, in funzione del tipo di attività, il nulla osta di sicurezza delle imprese può essere rilasciato prima della firma della sovvenzione. L'autorità erogatrice valuterà la necessità di nulla osta caso per caso e ne stabilirà la data di rilascio durante la preparazione della sovvenzione. **In nessun caso** sarà firmata una convenzione di sovvenzione finché almeno uno dei beneficiari di un consorzio non è in possesso di un nulla osta di sicurezza delle imprese.

Alla convenzione di sovvenzione possono essere aggiunte ulteriori raccomandazioni di sicurezza sotto forma di deliverable (*ad es. creare un gruppo consultivo in materia di sicurezza, limitare il livello di dettaglio, usare uno scenario fittizio, escludere l'uso di informazioni classificate ecc.*).

I beneficiari devono garantire che i progetti non sono soggetti a requisiti di sicurezza nazionali/di paesi terzi che possano avere un impatto sull'attuazione o mettere in discussione l'aggiudicazione della sovvenzione (*ad es. limitazioni tecnologiche, classifica di sicurezza nazionale ecc.*). L'autorità erogatrice deve essere informata immediatamente di possibili questioni inerenti alla sicurezza.

[OPZIONE supplementare per CQP: per i partenariati quadro è possibile che siano sottoposte a controllo di sicurezza sia le domande di partenariato quadro che le domande di sovvenzione.]

([1]) Cfr. decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

ALLEGATO II

CLAUSOLE STANDARD DELLA CONVENZIONE DI SOVVENZIONE

(da adattare alla convenzione di sovvenzione utilizzata)

13.2 Sicurezza - Informazioni classificate

Le parti devono trattare le informazioni classificate (UE o nazionali) conformemente al diritto dell'UE o nazionale applicabile sulle informazioni classificate [in particolare la decisione (UE, Euratom) 2015/444 della Commissione ([1]) e le relative norme di attuazione].

Le norme di sicurezza specifiche (se del caso) sono stabilite all'allegato 5.

ALLEGATO 5

Sicurezza — Informazioni classificate UE

[*OPZIONE per azioni con informazioni classificate UE (standard):* le informazioni classificate UE usate o generate dall'azione devono essere trattate conformemente alla guida alle classifiche di sicurezza (SCG) e alla lettera sugli aspetti di sicurezza (SAL) di cui all'allegato 1 e alla decisione (UE, Euratom) 2015/444 e relative norme di attuazione, fino alla loro declassificazione.

I deliverable contenenti informazioni classificate UE devono essere presentati conformemente a procedure speciali convenute con l'autorità erogatrice.

Le azioni che comportano informazioni classificate UE possono essere subappaltate solo previa autorizzazione scritta espressa dell'autorità erogatrice e solo a soggetti stabiliti in uno Stato membro dell'UE o in un paese non UE che abbia concluso un accordo sulla sicurezza delle informazioni con l'UE (o un accordo amministrativo con la Commissione).

Le informazioni classificate UE non possono essere divulgate a terzi (compresi i partecipanti all'attuazione dell'azione) senza previa autorizzazione espressa scritta dell'autorità erogatrice.]

([1]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

ALLEGATO III

[Allegato IV (del ……)]

LETTERA SUGLI ASPETTI DI SICUREZZA (SAL) ([1])

[Modello]

([1]) Il presente modello di SAL si applica quando la Commissione è considerata l'originatore delle informazioni classificate create e trattate per l'esecuzione della convenzione di sovvenzione. Se l'originatore di informazioni classificate create e trattate per l'esecuzione della convenzione di sovvenzione non è la Commissione e se gli Stati membri che partecipano alla sovvenzione istituiscono uno specifico quadro di sicurezza, possono applicarsi altri modelli di SAL.

Appendice A

REQUISITI DI SICUREZZA

Nella lettera sugli aspetti di sicurezza (SAL) l'autorità erogatrice deve includere i requisiti di sicurezza indicati di seguito. È possibile che alcune clausole non si applichino alla convenzione di sovvenzione, nel qual caso sono indicate tra parentesi quadre.

L'elenco delle clausole non è esaustivo. Possono essere aggiunte ulteriori clausole in funzione della natura della sovvenzione classificata.

CONDIZIONI GENERALI [*N.B.: applicabili a tutte le convenzioni di sovvenzione classificate*]

1. La presente lettera sugli aspetti di sicurezza (SAL) è parte integrante della convenzione di sovvenzione classificata [o del subcontratto classificato] e descrive i requisiti di sicurezza specifici della convenzione. L'inosservanza di detti requisiti può costituire motivo sufficiente per porre fine alla convenzione di sovvenzione.

2. I beneficiari della sovvenzione sono soggetti a tutti gli obblighi previsti dalla decisione (UE, Euratom) 2015/444 della Commissione ([2]) (di seguito «decisione 2015/444») e relative norme di attuazione ([3]). Se riscontra un problema di applicazione del quadro giuridico applicabile in uno Stato membro, il beneficiario della sovvenzione deve riferirlo all'autorità di sicurezza della Commissione e all'autorità di sicurezza nazionale (NSA) o all'autorità di sicurezza designata (DSA).

3. Le informazioni classificate generate durante l'esecuzione della convenzione di sovvenzione devono essere contrassegnate come informazioni classificate UE (ICUE) al livello di classifica di sicurezza stabilito nella guida alle classifiche di sicurezza (SCG) di cui all'appendice B della presente lettera. Lo scostamento dal livello di classifica di sicurezza stabilito dalla SCG è consentito solo previa autorizzazione scritta dell'autorità erogatrice.

4. Esercita i diritti dell'originatore delle ICUE create e trattate per l'esecuzione della convenzione di sovvenzione la Commissione in qualità di autorità erogatrice.

5. Senza il consenso scritto dell'autorità erogatrice il beneficiario o il subcontraente non possono fare uso delle informazioni o dei materiali messi a disposizione dall'autorità erogatrice o prodotti per suo conto per fini diversi da quelli della convenzione di sovvenzione.

6. Se è necessario un nulla osta di sicurezza delle imprese (FSC) per l'esecuzione di una convenzione di sovvenzione, il beneficiario deve chiedere all'autorità erogatrice di provvedere alla domanda di FSC.

7. Il beneficiario deve indagare su tutte le violazioni della sicurezza relative alle ICUE e riferirne all'autorità erogatrice appena possibile. Il beneficiario o il subcontraente deve riferire immediatamente alla propria NSA o DSA e, se le disposizioni legislative e regolamentari nazionali lo permettono, all'autorità di sicurezza della Commissione tutti i casi in cui è noto o vi è motivo di sospettare che le ICUE fornite o generate nel quadro della convenzione di sovvenzione sono state smarrite o sono state comunicate a persone non autorizzate.

([2]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

([3]) L'autorità erogatrice dovrà inserire i riferimenti dopo l'adozione delle norme di attuazione.

8. Al termine della convenzione di sovvenzione il beneficiario o il subcontraente deve restituire il prima possibile all'autorità erogatrice tutte le ICUE in suo possesso. Ove possibile, il beneficiario o il subcontraente può distruggere le ICUE anziché restituirle. A tal fine deve attenersi alle disposizioni legislative e regolamentari del paese in cui ha sede, previo accordo dell'autorità di sicurezza della Commissione, e conformemente alle istruzioni di quest'ultima. Le ICUE devono essere distrutte in modo tale da non poter essere ricostruite né totalmente né parzialmente.

9. Se il beneficiario o il subcontraente è autorizzato a conservare le ICUE dopo la risoluzione o la conclusione della convenzione di sovvenzione, le ICUE devono continuare ad essere protette conformemente alla decisione 2015/444 e alle relative norme di attuazione ([4]).

10. Il trattamento, l'elaborazione e la trasmissione elettronici delle ICUE avvengono nel rispetto delle disposizioni dei capi 5 e 6 della decisione 2015/444. Queste prevedono tra l'altro l'obbligo di sottoporre ad accreditamento i sistemi di comunicazione e informazione di proprietà del beneficiario e utilizzati per il trattamento delle ICUE ai fini della convenzione di sovvenzione (di seguito «CIS del beneficiario») ([5]); l'obbligo di proteggere la trasmissione elettronica delle ICUE mediante prodotti crittografici approvati a norma dell'articolo 36, paragrafo 4, della decisione 2015/444 e l'obbligo di attuare misure di sicurezza TEMPEST a norma dell'articolo 36, paragrafo 6, della decisione 2015/444.

11. Il beneficiario o il subcontraente predispone piani di emergenza (BCP) per proteggere le ICUE trattate nell'esecuzione della convenzione di sovvenzione classificata in situazioni di emergenza e mette in atto misure di prevenzione e recupero per ridurre al minimo l'impatto degli incidenti in relazione al trattamento e alla conservazione delle ICUE. Il beneficiario o il subcontraente deve comunicare il suo BCP all'autorità erogatrice.

CONVENZIONI DI SOVVENZIONE CHE RICHIEDONO L'ACCESSO A INFORMAZIONI CLASSIFICATE RESTREINT UE/EU RESTRICTED

12. In linea di principio ai fini della conformità alla convenzione di sovvenzione non è richiesto il nulla osta di sicurezza del personale (PSC) ([6]). Tuttavia le informazioni o i materiali classificati RESTREINT UE/EU RESTRICTED devono essere accessibili solo al personale del beneficiario che ha bisogno di dette informazioni per eseguire la convenzione di sovvenzione (*principio della necessità di conoscere*), che è stato istruito dal responsabile della sicurezza del beneficiario sulle sue responsabilità e sulle conseguenze di compromissioni o violazioni della sicurezza di dette informazioni e che ha riconosciuto per iscritto le conseguenze della mancata protezione delle ICUE.

13. Senza il consenso scritto dell'autorità erogatrice, il beneficiario o il subcontraente non può dare l'accesso alle informazioni o al materiale classificati RESTREINT UE/EU RESTRICTED a soggetti diversi dal proprio personale che ha necessità di conoscere.

14. Il beneficiario o il subcontraente deve mantenere i contrassegni di classifica di sicurezza delle informazioni classificate generate o trasmesse durante l'esecuzione della convenzione di sovvenzione e non può declassificarle senza il consenso scritto dell'autorità erogatrice.

15. Le informazioni o i materiali classificati RESTREINT UE/EU RESTRICTED, quando non utilizzati, devono essere conservati in mobili da ufficio chiusi a chiave. Durante il trasporto i documenti devono essere contenuti in una busta opaca. Il latore deve sempre portare con sé i documenti, che non possono essere aperti durante il trasporto.

([4]) L'autorità erogatrice dovrà inserire i riferimenti dopo l'adozione delle norme di attuazione.

([5]) La parte che chiede l'accreditamento dovrà presentare all'autorità erogatrice una dichiarazione di conformità, tramite l'autorità di sicurezza della Commissione e in coordinamento con l'autorità nazionale di accreditamento in materia di sicurezza (SAA).

([6]) Se i beneficiari provengono da Stati membri che richiedono PSC e/o FSC per le sovvenzioni classificate RESTREINT UE/EU RESTRICTED, l'autorità erogatrice elenca nella SAL tali requisiti per i beneficiari in questione.

16. Il beneficiario o il subcontraente può trasmettere i documenti classificati RESTREINT UE/EU RESTRICTED all'autorità erogatrice tramite corriere commerciale, servizio postale, trasporto a mano o mediante mezzi elettronici. A tal fine il beneficiario o il subcontraente deve attenersi alle istruzioni di sicurezza del programma (o progetto) (PSI) impartite dalla Commissione e/o alle norme di attuazione della Commissione in materia di sicurezza industriale per quanto riguarda le convenzioni di sovvenzione classificate ([7]).

17. Quando non più necessari, i documenti classificati RESTREINT UE/EU RESTRICTED devono essere distrutti in modo tale da non poter essere ricostruiti né totalmente né parzialmente.

18. L'accreditamento di sicurezza del CIS del beneficiario che tratta le ICUE a livello RESTREINT UE/EU RESTRICTED e di tutte le relative interconnessioni può essere delegato al responsabile della sicurezza del beneficiario se consentito dalle disposizioni legislative e regolamentari nazionali. Nei casi in cui l'accreditamento viene delegato, le NSA, le DSA o le autorità di accreditamento in materia di sicurezza (SAA) restano responsabili della protezione delle informazioni RESTREINT UE/EU RESTRICTED trattate dal beneficiario e conservano il diritto di ispezionare le misure di sicurezza che questi ha adottato. Inoltre il beneficiario fornisce all'autorità erogatrice e se richiesto dalle disposizioni legislative e regolamentari nazionali alla SAA nazionale competente, una dichiarazione di conformità in cui si certifica che il CIS del beneficiario e le relative interconnessioni sono stati accreditati per il trattamento di ICUE di livello RESTREINT UE/EU RESTRICTED.

TRATTAMENTO DELLE INFORMAZIONI CLASSIFICATE RESTREINT UE/EU RESTRICTED NEI SISTEMI DI COMUNICAZIONE E INFORMAZIONE (CIS)

19. I requisiti minimi per i CIS che trattano informazioni classificate RESTREINT UE/EU RESTRICTED sono stabiliti nell'appendice E della presente SAL.

CONDIZIONI ALLE QUALI IL BENEFICIARIO PUÒ SUBAPPALTARE

20. Prima di subappaltare una parte di una convenzione di sovvenzione classificata, il beneficiario deve ottenere l'autorizzazione dell'autorità erogatrice.

21. Non è possibile subappaltare a un soggetto registrato in un paese non UE o appartenente a un'organizzazione internazionale se tale paese o organizzazione non hanno concluso un accordo sulla sicurezza delle informazioni con l'UE o un accordo amministrativo con la Commissione.

22. Se il beneficiario ha concluso un subcontratto, le disposizioni in materia di sicurezza del contratto si applicano *mutatis mutandis* al o ai subcontraenti e al relativo personale. In questi casi spetta al beneficiario garantire che tutti i subcontraenti applichino a loro volta le predette disposizioni ai propri subcontratti. Per garantire un adeguato controllo della sicurezza, le NSA e/o le DSA del beneficiario e del subcontraente sono informate dall'autorità di sicurezza della Commissione della conclusione di tutti i subcontratti connessi classificati CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET. Se del caso, alle NSA e/o alle DSA del beneficiario e del subcontraente è trasmessa copia delle disposizioni di sicurezza specifiche per i subcontratti. Le NSA e le DSA che richiedono la notifica delle disposizioni di sicurezza delle convenzioni di sovvenzione classificate RESTREINT UE/EU RESTRICTED sono elencate nell'allegato delle norme di attuazione della Commissione in materia di sicurezza industriale per quanto riguarda le convenzioni di sovvenzione classificate ([8]).

23. Il beneficiario non può comunicare le ICUE al subcontraente senza la previa approvazione scritta dell'autorità erogatrice. Se ai subcontraenti devono essere inviate ICUE frequentemente o abitualmente, l'autorità erogatrice può dare l'approvazione per un periodo di tempo specifico (ad es. 12 mesi) o per la durata del subcontratto.

([7]) L'autorità erogatrice dovrà inserire i riferimenti dopo l'adozione delle norme di attuazione.
([8]) L'autorità erogatrice dovrà inserire i riferimenti dopo l'adozione delle norme di attuazione.

VISITE

Se per le visite riguardanti informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET deve essere applicata la procedura per la richiesta di visita (RFV) standard, l'autorità erogatrice deve includere le clausole 24, 25 e 26 e sopprimere la clausola 27. Se le visite che comportano informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono organizzate direttamente tra la struttura che invia e la struttura che riceve i visitatori, l'autorità erogatrice deve sopprimere le clausole 25 e 26 e includere unicamente la clausola 27.

24. Le visite che comportano l'accesso o il potenziale accesso a informazioni classificate RESTREINT UE/EU RESTRICTED sono organizzate direttamente tra la struttura che invia e la struttura che riceve i visitatori senza dover seguire la procedura di cui alle successive clausole da 25 a 27.

[25. Le visite che comportano l'accesso o il potenziale accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono soggette alla procedura seguente:

a) il responsabile della sicurezza della struttura che invia il visitatore compila tutte le parti pertinenti del modulo RFV (appendice C) e presenta la richiesta all'NSA o alla DSA della struttura;

b) l'NSA o la DSA della struttura che invia il visitatore deve confermare il PSC del visitatore prima di inoltrare l'RFV all'NSA o alla DSA della struttura ospitante (o all'autorità di sicurezza della Commissione se la visita ha luogo nei locali dell'autorità erogatrice);

c) il responsabile della sicurezza della struttura che invia il visitatore deve poi acquisire dalla propria NSA o DSA la risposta dell'NSA o DSA della struttura ospitante (o dell'autorità di sicurezza della Commissione) di approvazione o di rigetto dell'RFV;

d) l'RFV è considerata approvata se non vengono sollevate obiezioni fino ai cinque giorni lavorativi precedenti la data della visita.]

[26. Prima di dare ai visitatori accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, la struttura ospitante deve aver ottenuto l'autorizzazione dalla propria NSA o DSA.]

[27. Le visite che comportano l'accesso o il potenziale accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono organizzate direttamente tra la struttura che invia e la struttura che riceve i visitatori (un esempio di modulo utilizzabile a questo scopo figura nell'appendice C).]

28. I visitatori devono dimostrare la propria identità all'arrivo presso la struttura ospitante presentando una carta d'identità o un passaporto validi.

29. La struttura ospitante provvede alla tenuta dei registri di tutti i visitatori, in cui devono essere iscritti nome e cognome dei visitatori, organizzazione che rappresentano, data di scadenza del PSC (se applicabile), data della visita e nome e cognome della persona o delle persone visitate. Fatte salve le norme europee in materia di protezione dei dati, tali registri devono essere conservati per un periodo non inferiore a cinque anni o conformemente alle norme e ai regolamenti nazionali, a seconda dei casi.

VISITE DI VALUTAZIONE

30. L'autorità di sicurezza della Commissione può, in collaborazione con le pertinenti NSA o DSA, effettuare visite presso le strutture dei beneficiari o dei subcontraenti per verificare il rispetto dei requisiti di sicurezza per il trattamento delle ICUE.

GUIDA ALLE CLASSIFICHE DI SICUREZZA

31. La guida alle classifiche di sicurezza (SCG) contiene l'elenco di tutti gli elementi della convenzione di sovvenzione classificati o da classificare nel corso dell'esecuzione della convenzione, le relative norme e le specifiche dei livelli delle classifiche di sicurezza applicabili. L'SCG è parte integrante del presente contratto e figura nell'appendice B del presente allegato.

Appendice B

GUIDA ALLE CLASSIFICHE DI SICUREZZA

[testo specifico da adattare in funzione dell'oggetto della convenzione di sovvenzione]

Appendice C

REQUEST FOR VISIT (MODEL)

ISTRUZIONI DETTAGLIATE PER LA COMPILAZIONE DELLA RICHIESTA DI VISITA

(La richiesta deve essere presentata unicamente in inglese)

HEADING	Barrare le caselle per il tipo di visita e il tipo di informazione e indicare il numero di siti da visitare e il numero di visitatori.
4. **ADMINISTRATIVE DATA**	Da compilare a cura dell'NSA/DSA richiedente.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Indicare il nome completo e l'indirizzo postale. Indicare la città, lo Stato e il codice postale, a seconda dei casi.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Indicare il nome completo e l'indirizzo postale. Indicare la città, lo Stato, il codice postale, il numero di telex o di fax (se del caso), il numero di telefono e l'email. Indicare il nome, il numero di telefono/fax e l'email del principale punto di contatto o della persona con cui è stato fissato l'appuntamento per la visita. Osservazioni: 1) è importante indicare il codice postale corretto, perché una società può avere diverse strutture; 2) se la richiesta è presentata a mano, si può utilizzare l'allegato 1 quando occorre visitare due o più strutture in relazione allo stesso oggetto. Quando si utilizza un allegato, al punto 3 occorre inserire: «SEE ANNEX 1, NUMBER OF FAC.:...» (indicando il numero di strutture).
7. **DATES OF VISIT**	Indicare la data o il periodo effettivi (da data a data) della visita nel formato «giorno - mese - anno». Se del caso, indicare tra parentesi una data o un periodo alternativi.
8. **TYPE OF INITIATIVE**	Specificare se la visita è stata promossa dall'organizzazione o dalla struttura richiedente o se è su invito della struttura da visitare.
9. **THE VISIT RELATES TO:**	Indicare il nome completo del progetto, del contratto o dell'invito utilizzando solo abbreviazioni comunemente usate.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Breve descrizione dei motivi della visita. Non utilizzare abbreviazioni non spiegate. Osservazioni: in caso di visite ricorrenti, in questa voce iniziare la frase con le parole «Recurring visits» (ad es. «Recurring visits to discuss_____»).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Indicare SECRET UE/EU SECRET (S-UE/EU-S) o CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), a seconda dei casi.

12. **PARTICULARS OF VISITOR**	Nota bene: quando alla visita partecipano più di due visitatori, utilizzare l'allegato 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	In questa voce indicare il nome e il cognome, il numero di telefono, il numero di fax e l'indirizzo email del responsabile della sicurezza della struttura richiedente.
14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL**	Campo da compilare a cura dell'autorità di certificazione. Note per l'autorità di certificazione: a. indicare il nome, l'indirizzo, il numero di telefono e di fax e l'email (possono essere prestampati); b. apporre firma e timbro (se del caso).
15. **REQUESTING SECURITY AUTHORITY**	Campo da compilare a cura dell'NSA/DSA. Nota per l'NSA/DSA: a. indicare il nome, l'indirizzo, il numero di telefono e di fax e l'email (possono essere prestampati); b. apporre firma e timbro (se del caso).

Devono essere compilati tutti i campi e il modulo deve essere trasmesso mediante i canali di comunicazione tra amministrazioni ([9]).

REQUEST FOR VISIT

(MODEL)

TO: _____

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

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

([9]) Se è stato concordato che le visite che comportano l'accesso o il potenziale accesso a ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET possono essere organizzate direttamente, il modulo compilato può essere presentato direttamente al responsabile della sicurezza della struttura da visitare.

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

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

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

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

8. **TYPE OF INITIATIVE:**

□ Initiated by requesting organisation or facility

□ By invitation of the facility to be visited

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

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

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

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

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

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

STAMP

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

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

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE:

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

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

<Spazio riservato alle norme applicabili di protezione dei dati personali e al link alle informazioni obbligatorie a beneficio dell'interessato, ad es. le modalità di applicazione dell'articolo 13 del regolamento generale sulla protezione dei dati ([10]).>

([10]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

<Spazio riservato alle norme applicabili di protezione dei dati personali e al link alle informazioni obbligatorie a beneficio dell'interessato, ad es. le modalità di applicazione dell'articolo 13 del regolamento generale sulla protezione dei dati ([11]).>

([11]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
1. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
2. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION: ***(Continue as required)***

<Spazio riservato alle norme applicabili di protezione dei dati personali e al link alle informazioni obbligatorie a beneficio dell'interessato, ad es. le modalità di applicazione dell'articolo 13 del regolamento generale sulla protezione dei dati ([12]).>

([12]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

Appendice D

MODULO DI INFORMAZIONE SUL NULLA OSTA DI SICUREZZA DELLE IMPRESE (FSCIS) (MODELLO)

1. **INTRODUZIONE**

1.1. Il modulo allegato è un modello di modulo di informazione sul nulla osta di sicurezza delle imprese (FSCIS) per lo scambio rapido di informazioni tra l'autorità di sicurezza nazionale (NSA) o l'autorità di sicurezza designata (DSA), altre autorità di sicurezza nazionali competenti e l'autorità di sicurezza della Commissione (che agisce per conto delle autorità che erogano le sovvenzioni) sul nulla osta di sicurezza delle imprese (FSC) di una struttura partecipante alla domanda e all'attuazione di sovvenzioni o subcontratti classificati.

1.2. L'FSCIS è valido solo se timbrato dall'NSA/DSA competente o da altra autorità competente.

1.3. L'FSCIS è composto di una sezione relativa alla richiesta e una relativa alla risposta, e può essere utilizzato per le summenzionate finalità o per altri scopi per i quali è richiesto l'FSC di una specifica struttura. Il motivo della richiesta deve essere indicato dall'NSA o dalla DSA richiedente nel campo 7 della sezione relativa alla richiesta.

1.4. Le informazioni contenute nell'FSCIS non sono di norma classificate; pertanto l'invio dell'FSCIS tra NSA/DSA/Commissione andrebbe di preferenza effettuato mediante mezzi elettronici.

1.5. Le NSA/DSA dovrebbero compiere ogni sforzo per rispondere alla richiesta di FSCIS entro dieci giorni lavorativi.

1.6. In caso di trasferimento di informazioni classificate o di aggiudicazione di una sovvenzione o subcontratto in relazione a tale assicurazione, l'NSA o la DSA emittente devono essere informate.

Procedure e istruzioni per l'uso del modulo di informazione sul nulla osta di sicurezza delle imprese (FSCIS)

Le istruzioni dettagliate che seguono sono rivolte all'NSA o alla DSA o all'autorità erogatrice e all'autorità di sicurezza della Commissione che compila l'FSCIS. La richiesta dovrebbe preferibilmente essere dattiloscritta in stampatello.

INTESTAZIONE	Il richiedente inserisce il nome completo dell'NSA/DSA e del paese.
1. **TIPO DI RICHIESTA**	L'autorità erogatrice richiedente barra la casella corrispondente al tipo di richiesta FSCIS. Indicare il livello di nulla osta di sicurezza oggetto della richiesta. Utilizzare le seguenti abbreviazioni: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = sistemi di comunicazione e informazione per il trattamento delle informazioni classificate
2. **INFORMAZIONI SUL RICHIEDENTE**	I campi da 1 a 6 non necessitano spiegazioni. Nel campo 4 utilizzare il codice paese standard a due lettere. Il campo 5 è facoltativo.
3. **MOTIVO DELLA RICHIESTA**	Indicare il motivo specifico della richiesta, inserire i riferimenti del progetto, il numero dell'invito o della sovvenzione. Specificare il fabbisogno di capacità di stoccaggio, il livello di classifica del CIS ecc. Indicare la data di ogni termine/scadenza/aggiudicazione che può influire sulla finalizzazione dell'FSC.

4. **NSA/DSA RICHIEDENTE**	Indicare il nome del richiedente effettivo (per conto dell'NSA/DSA) e la data della richiesta in formato numerico (gg/mm/aaaa).
5. **SEZIONE RELATIVA ALLA RISPOSTA**	Campi 1-5: selezionare i campi appropriati. Campo 2: se l'FSC è in lavorazione, si raccomanda di fornire al richiedente un'indicazione dei tempi di trattazione necessari (se noti). Campo 6: a) sebbene la convalida vari da un paese all'altro o persino da una struttura all'altra, si raccomanda di indicare la data di scadenza dell'FSC; b) se la data di scadenza dell'assicurazione in relazione all'FSC è indeterminata, sbarrare questo campo; c) conformemente alle norme e ai regolamenti nazionali rispettivi spetta al richiedente ovvero al beneficiario o al subcontraente presentare domanda di rinnovo dell'FSC.
6. **OSSERVAZIONI**	Campo utilizzabile per inserire ulteriori informazioni relative all'FSC, alla struttura o alle voci precedenti.
7. **NSA/DSA EMITTENTE**	Indicare il nome dell'autorità che ha trasmesso le informazioni (per conto dell'NSA/DSA) e la data della risposta in formato numerico (gg/mm/aaaa).

MODULO DI INFORMAZIONE SUL NULLA OSTA DI SICUREZZA DELLE IMPRESE (FSCIS)(MODELLO)

Devono essere compilati tutti i campi e il modulo deve essere trasmesso mediante i canali di comunicazione tra amministrazioni o tra amministrazioni e organizzazioni internazionali.

RICHIESTA DI ASSICURAZIONE IN RELAZIONE AL NULLA OSTA DI SICUREZZA DELLE IMPRESE

A: _____

(Nome del paese dell'NSA/DSA)

Completare le caselle di risposta, a seconda del caso:

[ ] Fornire un'assicurazione in relazione all'FSC di livello: [ ] S-UE/EU-S [ ] C-UE/EU-C

della struttura indicata in basso

[ ] anche per quanto riguarda la protezione di informazioni/materiali classificati

[ ] anche per quanto riguarda i sistemi di comunicazione e informazione (CIS) per il trattamento delle informazioni classificate

[ ] Avviare, direttamente o su richiesta di un beneficiario o subcontraente, la procedura per il rilascio dell'FSC fino al livello di ..... incluso, con il livello di protezione ..... e il livello del CIS ..... se la struttura non dispone attualmente di detti livelli di capacità.

Confermare l'esattezza dei dati sulla struttura indicata in basso e fornire rettifiche/aggiunte se necessario.

1. Nome completo della struttura:	Rettifiche/aggiunte:
.....	.....
2. Indirizzo completo della struttura:	
.....	.....
3. Indirizzo postale (se diverso da 2)	
.....	.....
4. Codice postale/città/Stato	
.....	.....
5. Nome del responsabile della sicurezza	
.....	
.....	
6. Telefono/fax/email del responsabile della sicurezza	
.....	.....

7. La presente richiesta è presentata per i seguenti motivi: (fornire i dati della fase precontrattuale (di selezione delle proposte), della sovvenzione o del subcontratto, del programma/progetto ecc.)

.....

NSA/DSA/autorità erogatrice richiedente: Data (gg/mm/aaaa).....
Nome: .....

Risposta (entro 10 giorni lavorativi)

Si certifica quanto segue:

1. [ ] La summenzionata struttura è in possesso di un FSC fino al livello [ ] S-UE/EU-S incluso

   [ ] C-UE/EU-C incluso.

2. La summenzionata struttura è in grado di proteggere le informazioni/i materiali classificati:

   [ ] sì, livello: ..... [ ] no.

3. La summenzionata struttura dispone di un CIS accreditato/autorizzato:

   [ ] sì, livello: ..... [ ] no.

4. [ ] In relazione alla predetta richiesta è stata avviata la procedura di rilascio dell'FSC. Sarete informati del rilascio o del diniego dell'FSC.

5. [ ] La summenzionata struttura non è in possesso di FSC.

6. La presente assicurazione in relazione all'FSC scade il: ..... (*gg/mm/aaaa*), o come altrimenti raccomandato dall'NSA/DSA. Sarete informati in caso di invalidamento anticipato o di modifica delle informazioni riportate in alto.

7. Osservazioni:
   .....

NSA/DSA emittente Nome: ..... Data (gg/mm/aaaa) .....

<Spazio riservato alle norme applicabili di protezione dei dati personali e al link alle informazioni obbligatorie a beneficio dell'interessato, ad es. le modalità di applicazione dell'articolo 13 del regolamento generale sulla protezione dei dati ([13]).>

([13]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

Appendice E

Requisiti minimi per la protezione delle ICUE in formato elettronico di livello RESTREINT UE/EU RESTRICTED trattate nel CIS del beneficiario

Aspetti generali

1. Il beneficiario deve assicurare che la protezione delle informazioni RESTREINT UE/EU RESTRICTED sia conforme ai requisiti minimi di sicurezza previsti dalla presente clausola di sicurezza e a ogni altro ulteriore requisito raccomandato dall'autorità erogatrice o, se del caso, dall'autorità nazionale di sicurezza (NSA) o dall'autorità di sicurezza designata (DSA).

2. Spetta al beneficiario attuare i requisiti di sicurezza indicati nel presente documento.

3. Ai fini del presente documento, per sistema di comunicazione e informazione (CIS) si intendono tutte le apparecchiature utilizzate per trattare, conservare e trasmettere le ICUE, tra cui terminali, stampanti, fotocopiatrici, fax, server, sistemi di gestione della rete, unità di controllo della rete, unità di controllo delle comunicazioni, laptop, notebook, tablet, smartphone e supporti di memoria removibili, come chiavette USB, CD, carte SD ecc.

4. Le apparecchiature speciali, quali i prodotti crittografici, devono essere protette conformemente a specifiche procedure operative di sicurezza (SecOP) dedicate.

5. I beneficiari devono istituire una struttura responsabile della gestione della sicurezza del CIS che tratta informazioni classificate RESTREINT UE/EU RESTRICTED e nominare un responsabile della sicurezza della struttura stessa.

6. Per la conservazione o l'elaborazione delle informazioni RESTREINT UE/EU RESTRICTED non è consentito l'uso di soluzioni informatiche (hardware, software o servizi) di proprietà privata del personale del beneficiario.

7. L'accreditamento del CIS del beneficiario che tratta informazioni classificate RESTREINT UE/EU RESTRICTED deve essere approvato dall'autorità di accreditamento in materia di sicurezza (SAA) dello Stato membro interessato, oppure delegato al responsabile della sicurezza del beneficiario secondo quanto consentito dalle disposizioni legislative e regolamentari nazionali.

8. Solo le informazioni classificate RESTREINT UE/EU RESTRICTED cifrate utilizzando prodotti crittografici approvati possono essere trattate, conservate o trasmesse (via cavo o senza fili) come qualsiasi altra informazione non classificata nel quadro della convenzione di sovvenzione. I predetti prodotti crittografici devono essere approvati dall'UE o da uno Stato membro.

9. Le strutture esterne coinvolte nelle attività di manutenzione/riparazione devono essere contrattualmente obbligate a rispettare le disposizioni applicabili in materia di trattamento delle informazioni classificate RESTREINT UE/EU RESTRICTED specificate nel presente documento.

10. Su richiesta dell'autorità erogatrice o dell'NSA, DSA o SAA competente, il beneficiario deve produrre elementi a comprova del rispetto della clausola di sicurezza della convenzione di sovvenzione. Qualora per verificare la conformità ai predetti requisiti siano richiesti anche l'audit e l'ispezione dei processi e delle strutture del beneficiario, questi consente ai rappresentanti dell'autorità erogatrice, dell'NSA, DSA o SAA o dell'autorità di sicurezza competente dell'UE di procedere all'audit e all'ispezione.

Sicurezza materiale

11. Le zone in cui i CIS sono usati per visualizzare, conservare, trattare o trasmettere informazioni RESTREINT UE/EU RESTRICTED o le zone che ospitano i server, i sistemi di gestione della rete, le unità di controllo della rete e le unità di controllo delle comunicazioni di tali CIS dovrebbero essere costituite come zone separate e controllate con adeguato sistema di controllo dell'accesso. L'accesso a queste zone separate e controllate dovrebbe essere riservato alle persone fisiche in possesso di specifica autorizzazione. Fatta salva la clausola 8, le apparecchiature di cui alla clausola 3 devono essere custodite in zone separate e controllate.

12. Devono essere attuati meccanismi e/o procedure di sicurezza per disciplinare l'introduzione o la connessione di supporti informatici removibili (quali USB, memorie di massa o CD-RW) a componenti del CIS.

Accesso al CIS

13. L'accesso al CIS del beneficiario che tratta ICUE è consentito sulla base dell'applicazione rigorosa del principio della necessità di conoscere e dell'autorizzazione del personale.

14. Tutti i CIS devono disporre di elenchi aggiornati degli utenti autorizzati. Tutti gli utenti devono essere autenticati all'inizio di ogni sessione di trattamento.

15. Le password, previste dalla maggior parte delle misure di sicurezza per l'identificazione e l'autenticazione, devono essere formate da almeno nove caratteri, tra cui caratteri numerici, caratteri «speciali» (se consentito dal sistema) e caratteri alfabetici. Le password devono essere modificate almeno ogni 180 giorni. Devono essere modificate il prima possibile se sono state compromesse o comunicate a persone non autorizzate, o se vi sono sospetti di compromissione o comunicazione.

16. Tutti i CIS devono disporre di controlli sull'accesso interno per impedire a utenti non autorizzati di accedere a informazioni classificate RESTREINT UE/EU RESTRICTED o di modificarle, o di modificare il sistema e i controlli di sicurezza. L'utente viene automaticamente disconnesso dal CIS se il suo terminale rimane inattivo per un tempo predefinito, oppure il CIS deve attivare un salvaschermo protetto da password dopo 15 minuti di inattività.

17. A ogni utente del CIS viene attribuito un account e un nome utente. Gli account devono essere automaticamente bloccati almeno dopo cinque tentativi di accesso errati.

18. Tutti gli utenti del CIS devono essere istruiti sulle proprie responsabilità e sulle procedure da seguire per proteggere le informazioni classificate RESTREINT UE/EU RESTRICTED nel CIS. Le responsabilità e le procedure da seguire devono essere documentate e accettate per iscritto dagli utenti.

19. Agli utenti e agli amministratori sono messe a disposizione le SecOP, le quali devono contenere la descrizione dei ruoli in materia di sicurezza e il relativo elenco di compiti, istruzioni e piani.

Registrazione, audit e risposta agli incidenti

20. Ogni accesso al CIS deve essere registrato.

21. Devono essere registrati i seguenti eventi:

    a) tutti i tentativi di connessione, sia riusciti che non riusciti;

    b) la disconnessione (anche per sessione scaduta, se del caso);

    c) la creazione, cancellazione o modifica dei diritti e dei privilegi di accesso;

    d) la creazione, cancellazione o modifica di password.

22. Per tutti gli eventi sopraelencati devono essere comunicate almeno le informazioni seguenti:

    a) tipo di evento;

    b) nome utente;

    c) data e ora;

    d) ID dispositivo.

23. Le registrazioni dovrebbero essere di ausilio al responsabile della sicurezza nell'esame dei potenziali incidenti di sicurezza. Possono inoltre essere utilizzate a supporto delle indagini giudiziarie in caso di incidente di sicurezza. Tutte le registrazioni relative alla sicurezza dovrebbero essere verificate periodicamente per individuare potenziali incidenti di sicurezza. Le registrazioni devono essere protette da cancellazioni o modifiche non autorizzate.

24. Il beneficiario deve disporre di una strategia di risposta consolidata per far fronte agli incidenti di sicurezza. Gli utenti e gli amministratori devono essere istruiti su come rispondere agli incidenti, su come segnalarli e su cosa fare in caso di emergenza.

25. La compromissione o sospetta compromissione di informazioni classificate RESTREINT UE/EU RESTRICTED devono essere segnalate all'autorità erogatrice. La segnalazione deve contenere la descrizione delle informazioni in questione e la descrizione delle circostanze della compromissione o della sospetta compromissione. Tutti gli utenti del CIS devono essere istruiti su come segnalare gli incidenti di sicurezza reali o presunti al responsabile della sicurezza.

Reti e interconnessioni

26. L'interconnessione del CIS del beneficiario che tratta informazioni classificate RESTREINT UE/EU RESTRICTED con un CIS non accreditato accresce in misura significativa le minacce per la sicurezza sia del CIS che delle informazioni RESTREINT UE/EU RESTRICTED trattate da tale CIS. Ciò riguarda in particolare internet e gli altri CIS pubblici o privati, quali gli altri CIS di proprietà del beneficiario o del subcontraente. In tal caso il beneficiario deve effettuare una valutazione del rischio per individuare le prescrizioni di sicurezza supplementari da applicare nel quadro del processo di accreditamento di sicurezza. Il beneficiario trasmette all'autorità erogatrice e se previsto dalle disposizioni legislative e regolamentari nazionali alla SAA competente una dichiarazione di conformità in cui si certifica che il CIS del contraente e le relative interconnessioni sono stati accreditati per il trattamento di ICUE di livello RESTREINT UE/EU RESTRICTED.

27. È vietato accedere a distanza ai servizi LAN da altri sistemi (ad es. accesso a distanza alle email e supporto a distanza del sistema), a meno che siano predisposte e approvate specifiche misure di sicurezza dall'autorità erogatrice e se previsto dalle disposizioni legislative e regolamentari nazionali dalla SAA competente.

Gestione della configurazione

28. Deve essere disponibile e soggetta a periodica manutenzione la configurazione dettagliata dell'hardware e del software, secondo quanto indicato nella documentazione di accreditamento/approvazione (compresi i diagrammi di sistema e di rete).

29. Il responsabile della sicurezza del beneficiario deve effettuare controlli sulla configurazione dell'hardware e del software per accertare che non sia stato introdotto hardware o software non autorizzato.

30. Le modifiche della configurazione del CIS del beneficiario devono essere valutate dal punto di vista delle implicazioni per la sicurezza e devono essere approvate dal responsabile della sicurezza e se previsto dalle disposizioni legislative e regolamentari nazionali dalla SAA.

31. Almeno una volta a trimestre il sistema deve essere ispezionato alla ricerca di eventuali vulnerabilità sotto il profilo della sicurezza. Deve essere installato e tenuto aggiornato il software per l'individuazione di malware. Se possibile detto software dovrebbe essere riconosciuto a livello nazionale o internazionale o essere uno standard ampiamente accettato nel settore.

32. Il beneficiario deve elaborare un piano di continuità operativa. Devono essere stabilite procedure di back-up che disciplinino i seguenti aspetti:

    a) frequenza dei backup;

    b) requisiti in materia di conservazione in loco (contenitori ignifughi) o all'esterno del sito;

    c) controllo dell'accesso autorizzato alle copie di back-up.

Sanitizzazione e distruzione

33. Per i CIS o per supporti informatici che in un qualsiasi momento hanno contenuto informazioni RESTREINT UE/EU RESTRICTED deve essere eseguita sull'intero sistema o sui supporti informatici prima del loro smaltimento la sanitizzazione seguente:

    a) la memoria flash (ad es. chiavette USB, carte SD, dischi a stato solido, dischi rigidi ibridi) deve essere sovrascritta almeno tre volte e poi verificata, per garantire che il contenuto originario non possa essere recuperato, o cancellata con un software di cancellazione approvato;

    b) i supporti magnetici (ad es. dischi rigidi) devono essere sovrascritti o smagnetizzati;

    c) i supporti ottici (ad es. CD e DVD) devono essere triturati o disintegrati;

    d) per ogni altro supporto dovrebbe essere consultata in merito ai requisiti di sicurezza da rispettare l'autorità erogatrice o se del caso l'NSA, la DSA o la SAA.

34. Le informazioni classificate RESTREINT UE/EU RESTRICTED devono essere sanitizzate su qualsiasi supporto informatico prima che i supporti siano consegnati a soggetti non autorizzati ad accedere a informazioni classificate RESTREINT UE/EU RESTRICTED (ad es. per la manutenzione).

ALLEGATO IV

Nulla osta di sicurezza dell'impresa e nulla osta di sicurezza del personale per i beneficiari o subcontraenti di sovvenzioni comportanti informazioni RESTREINT UE/EU RESTRICTED e NSA/DSA che richiedono la notifica di convenzioni di sovvenzione classificate a livello RESTREINT UE/EU RESTRICTED ([1])

Stato membro	FSC		Notifica all'NSA e/o alla DSA della convenzione di sovvenzione o del subcontratto che comporta informazioni R-UE/EU-R		PSC	
	SÌ	NO	SÌ	NO	SÌ	NO
Belgio		**X**		**X**		**X**
Bulgaria		**X**		**X**		**X**
Cechia		**X**		**X**		**X**
Danimarca	**X**		**X**		**X**	
Germania		**X**		**X**		**X**
Estonia	**X**		**X**			**X**
Irlanda		**X**		**X**		**X**
Grecia	**X**			**X**	**X**	
Spagna		**X**	**X**			**X**
Francia		**X**		**X**		**X**
Croazia		**X**	**X**			**X**
Italia		**X**	**X**			**X**
Cipro		**X**	**X**			**X**
Lettonia		**X**		**X**		**X**
Lituania	**X**		**X**			**X**
Lussemburgo	**X**		**X**		**X**	
Ungheria		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Paesi Bassi	**X** (solo per convenzioni di sovvenzione e subcontratti nel settore della difesa)		**X** (solo per convenzioni di sovvenzione e subcontratti nel settore della difesa)			**X**
Austria		**X**		**X**		**X**
Polonia		**X**		**X**		**X**

([1]) Le prescrizioni nazionali in materia di FSC/PSC e di notifica di convenzioni di sovvenzione che comportano informazioni RESTREINT UE/EU RESTRICTED non devono imporre obblighi supplementari agli altri Stati membri o ai beneficiari o subcontraenti sotto la loro giurisdizione.
NB: la notifica delle convenzioni di sovvenzione che comportano informazioni CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET è obbligatoria.

Portogallo		**X**		**X**		**X**
Romania		**X**		**X**		**X**
Slovenia	**X**		**X**			**X**
Slovacchia	**X**		**X**			**X**
Finlandia		**X**		**X**		**X**
Svezia		**X**		**X**		**X**

ALLEGATO V

ELENCO DEI SERVIZI DELLE AUTORITÀ DI SICUREZZA NAZIONALI/DELLE AUTORITÀ DI SICUREZZA DESIGNATE RESPONSABILI DELLA GESTIONE DELLE PROCEDURE RELATIVE ALLA SICUREZZA INDUSTRIALE

BELGIO

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

Tel.: +32 25014542 (Segretariato)

Fax: +32 25014596

Email: nvo-ans@diplobel.fed.be

BULGARIA

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

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

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

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

(Le predette autorità competenti effettuano gli accertamenti per il rilascio dell'FSC alle persone giuridiche che presentano offerte per la conclusione di un contratto classificato, e del PSC alle persone fisiche che danno attuazione ad un contratto classificato per le esigenze delle autorità stesse).

5. State Agency National Security (security service)

   45 Cherni Vrah Blvd.
   1407 Sofia

   Tel.: +359 28147109

   Fax: +359 29632188, +359 28147441

   Email: dans@dans.bg

(Il predetto servizio di sicurezza effettua gli accertamenti per il rilascio dell'FSC e del PSC a tutte le altre persone giuridiche e fisiche del paese che rispondono a un invito per un contratto classificato o una convenzione di sovvenzione classificata o danno attuazione ad un contratto classificato o ad una convenzione di sovvenzione classificata).

CECHIA

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

Tel.: +420 257283129

Email: sbr@nbu.cz

DANIMARCA

1. Politiets Efterretningstjeneste
   (Danish Security Intelligence Service)

   Klausdalsbrovej 1

   2860 Søborg

   Tel.: +45 33148888

   Fax: +45 33430190

2. Forsvarets Efterretningstjeneste
   (Danish Defence Intelligence Service)
   Kastellet 30
   2100 Copenhagen Ø

   Tel.: +45 33325566

   Fax: +45 33931320

GERMANIA

1. Per le questioni relative alla politica di sicurezza industriale, gli FSC, i programmi di trasporto (tranne materiale crittografico/CCI):
   Federal Ministry for Economic Affairs and Energy

   Industrial Security Division - RS3

   Villemombler Str. 76

   53123 Bonn

   Tel.: +49 228996154028

   Fax: +49 228996152676

   Email: dsagermany-rs3@bmwi.bund.de (email ufficio)

2. Per le richieste di visita standard da/presso imprese tedesche:

Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS2
Villemombler Str. 76
53123 Bonn

Tel.: +49 228996152401

Fax: +49 228996152603

Email: rs2-international@bmwi.bund.de (email ufficio)

3. Programmi di trasporto di materiale crittografico:

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

Tel.: +49 2289995826052

Fax: +49 228991095826052

Email: NDAEU@bsi.bund.de

ESTONIA

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

Tel.: +372 6939211

Fax: +372 6935001

Email: nsa@fis.gov.ee

IRLANDA

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

Tel.: +353 14082724

Email: nsa@dfa.ie

GRECIA

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

Tel.: +30 2106572022, +30 2106572178

Fax: +30 2106527612

Email: daa.industrial@hndgs.mil.gr

SPAGNA

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

Tel.: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

Email: nsa-sp@areatec.com

Per le informazioni sui programmi classificati: programas.ons@areatec.com

Per le questioni riguardanti i nulla osta di sicurezza del personale: hps.ons@areatec.com

Per i programmi di trasporto e le visite internazionali: sp-ivtco@areatec.com

FRANCIA

National Security Authority (NSA) (per le politiche e l'attuazione in settori diversi da quello della difesa)
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

Tel.: +33 171758193

Fax: +33 171758200

Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (per l'attuazione nel settore della difesa)
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

Tel.: +33 988670421

Email: per moduli e RFV in uscita: dga-ssdi.ai.fct@intradef.gouv.fr

per RFV in entrata: dga-ssdi.visit.fct@intradef.gouv.fr

CROAZIA

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

Tel.: +385 14681222

Fax: +385 14686049

Email: NSACroatia@uvns.hr

ITALIA

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

Tel.: +39 0661174266

Fax: +39 064885273

CIPRO

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Email: cynsa@mod.gov.cy

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

Tel.: +357 22807569, +357 22807764

Fax: +357 22302351

Email: cynsa@mod.gov.cy

LETTONIA

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

Tel.: +371 67025418, +371 67025463

Fax: +371 67025454

Email: ndi@sab.gov.lv, ndi@zd.gov.lv

LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Pilaitės pr. 19
LT-06264 Vilnius

Tel.: +370 70666128

Email: nsa@vsd.lt

LUSSEMBURGO

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

Tel.: +352 24782210

Email: ans@me.etat.lu

UNGHERIA

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

Tel.: +36 13911862

Fax: +36 13911889

Email: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010

+356 23952000

Fax: +356 21242406

Email: certification@mccaa.org.mt

PAESI BASSI

1. Ministry of the Interior and Kingdom Relations

   PO Box 20010
   2500 EA The Hague

   Tel.: +31 703204400

   Fax: +31 703200733

   Email: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

   Industrial Security Department

   PO Box 20701
   2500 ES The Hague

   Tel.: +31 704419407

   Fax: +31 703459189

   Email: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria

   Department I/10, Federal Office for Information Security

   Ballhausplatz 2
   10104 Vienna

   Tel.: +43 153115202594

   Email: isk@bka.gv.at

2. DSA in the military sphere:

   BMLV/Abwehramt

   Postfach 2000
   1030 Vienna

   Email: abwa@bmlvs.gv.at

POLONIA

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2 A
00-993 Warsaw

Tel.: +48 225857944

Fax: +48 225857443

Email: nsa@abw.gov.pl

PORTOGALLO

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

Tel.: +351 213031710

Fax: +351 213031711

Email: sind@gns.gov.pt, franco@gns.gov.pt

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Romanian NSA - ORNISS - National Registry Office for Classified Information
4th Mures Street
012275 Bucharest

Tel.: +40 212075115

Fax: +40 212245830

Email: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel.: +386 14781390

Fax: +386 14781399

Email: gp.uvtp@gov.si

SLOVACCHIA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava

Tel.: +421 268691111

Fax: +421 268691700

Email: podatelna@nbu.gov.sk

FINLANDIA

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

Email: NSA@formin.fi

SVEZIA

1. National Security Authority

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

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