DECISIONE (UE, Euratom) 2015/444 DELLA COMMISSIONE

del 13 marzo 2015

sulle norme di sicurezza per proteggere le informazioni classificate UE

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 protocollo n. 7 sui privilegi e le immunità dell'Unione europea allegato ai trattati, in particolare l'articolo 18,

considerando quanto segue:

(1) È necessario rivedere e aggiornare le disposizioni della Commissione in materia di sicurezza per la protezione delle informazioni classificate UE (ICUE), tenendo conto degli sviluppi istituzionali, organizzativi, operativi e tecnologici.

(2) La Commissione europea ha concluso accordi per la sicurezza delle proprie sedi principali con i governi di Belgio, Lussemburgo e Italia ([1]).

(3) La Commissione, il Consiglio e il Servizio europeo per l'azione esterna si impegnano ad applicare norme di sicurezza equivalenti per proteggere le ICUE.

(4) È importante associare, ove opportuno, il Parlamento europeo e altre istituzioni, organi o organismi dell'Unione a principi, norme e regole per proteggere le informazioni classificate che sono necessari per salvaguardare gli interessi dell'Unione e dei suoi Stati membri.

(5) Il rischio per le ICUE è gestito secondo una procedura. Tale procedura è volta a determinare i rischi noti per la sicurezza, a definire le misure di sicurezza per contenere tali rischi entro un livello accettabile conformemente ai principi fondamentali e alle norme minime stabiliti nella presente decisione, e ad applicare tali misure secondo il concetto di difesa in profondità. L'efficacia di tali misure è valutata costantemente.

(6) Alla Commissione, per «sicurezza materiale per la protezione di informazioni classificate» si intende l'applicazione di misure di protezione materiali e tecniche volte a impedire l'accesso non autorizzato alle ICUE.

(7) Per «gestione delle ICUE» si intende l'applicazione delle misure amministrative intese a controllare le ICUE per tutto il loro ciclo di vita, al fine di integrare le misure previste ai capi 2, 3 e 5 della presente decisione e in tal modo contribuire a scoraggiare e scoprire casi di compromissione o perdita intenzionale o accidentale di tali informazioni. Dette misure riguardano in particolare la creazione, l'archiviazione, la registrazione, la copiatura, la traduzione, il declassamento, la declassificazione, il trasporto e la distruzione di ICUE e integrano le norme generali della Commissione sulla gestione dei documenti [decisioni 2002/47/CE ([2]), CECA, Euratom e 2004/563/CE, Euratom ([3])].

([1]) Cfr. l'«Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité» del 31 dicembre 2004, l'«Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois» del 20 gennaio 2007, e l'«Accordo tra il governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale» del 22 luglio 1959.

([2]) Decisione 2002/47/CE, CECA, Euratom, della Commissione del 23 gennaio 2002, recante modificazione del suo regolamento interno (GU L 21 del 24.1.2002, pag. 23).

([3]) Decisione 2004/563/CE, Euratom della Commissione, del 7 luglio 2004, che modifica il suo regolamento interno (GU L 251 del 27.7.2004, pag. 9).

(8) Le disposizioni della presente decisione non pregiudicano:

a) il regolamento (Euratom) n. 3 ([1]);

b) il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([2]);

c) il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([3]);

d) il regolamento (CEE, Euratom) n. 354/83 del Consiglio ([4]),

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

PRINCIPI FONDAMENTALI E NORME MINIME DI SICUREZZA

Articolo 1

Definizioni

Ai fini della presente decisione si intende per:

1) «servizio della Commissione», direzioni generali, servizi della Commissione o gabinetti dei membri della Commissione;

2) «materiale crittografico (crypto)», algoritmi crittografici, moduli hardware e software crittografici e prodotti comprendenti dettagli di attuazione e documentazione associata e materiale di codifica;

3) «declassificazione», la soppressione di qualsiasi classifica di sicurezza;

4) «difesa in profondità», l'applicazione di una serie di misure di sicurezza organizzate come fasi multiple di difesa;

5) «documento», qualsiasi informazione registrata, a prescindere dalla sua forma o dalle sue caratteristiche materiali;

6) «declassamento», una riduzione del livello di classifica di sicurezza;

7) «trattamento» delle ICUE, qualsiasi azione di cui possono essere oggetto le ICUE nel loro ciclo di vita. Ciò comprende la loro creazione, registrazione, elaborazione, trasporto, declassamento, declassificazione e distruzione. In relazione ai sistemi di comunicazione e informazione (CIS) il trattamento comprende anche la raccolta, la visualizzazione, la trasmissione e la conservazione;

8) «detentore», una persona debitamente autorizzata con una necessità di conoscere stabilita, che detiene un elemento di ICUE ed è di conseguenza responsabile della sua protezione;

9) «norme di attuazione», l'insieme di norme o di comunicazioni di sicurezza adottate in conformità al capo 5 della decisione (UE, Euratom) 2015/443 della Commissione ([5]);

10) «materiale», qualsiasi mezzo, vettore di dati o elemento di macchinario o attrezzatura, sia sotto forma di prodotto finito sia in corso di lavorazione;

11) «originatore», un'istituzione, agenzia o organo dell'Unione, Stato membro, Stato terzo o organizzazione internazionale sotto la cui autorità sono state create e/o introdotte nelle strutture dell'Unione informazioni classificate;

12) «locali», beni immobili o assimilabili della Commissione;

([1]) Regolamento (Euratom) n. 3, del 31 luglio 1958, recante attuazione dell'articolo 24 del trattato che istituisce la Comunità europea dell'energia atomica (GU 17 del 6.10.1958, pag. 406/58).

([2]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

([3]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

([4]) Regolamento (CEE, Euratom) n. 354/83 del Consiglio, del 1º febbraio 1983, che rende accessibili al pubblico gli archivi storici della Comunità economica europea e della Comunità europea dell'energia atomica (GU L 43 del 15.2.1983, pag. 1).

([5]) Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (Cfr. pagina 41 della presente Gazzetta ufficiale).

13) «procedura di gestione del rischio di sicurezza», l'intera procedura che consiste nell'individuare, controllare e ridurre al minimo eventi incerti che possono incidere sulla sicurezza di un'organizzazione o di un qualsiasi sistema in uso. Essa contempla tutte le attività correlate al rischio, tra cui la valutazione, il trattamento, l'accettazione e la comunicazione;

14) «statuto», lo statuto dei funzionari dell'Unione europea e il regime applicabile agli altri agenti dell'Unione europea definiti dal regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([1]);

15) «minaccia», causa potenziale di un incidente indesiderato che può recar danno a un'organizzazione o a uno dei sistemi in uso; tali minacce possono essere accidentali o intenzionali (dolose) e sono caratterizzate da elementi di minaccia, potenziali obiettivi e metodologie d'attacco;

16) «vulnerabilità», una debolezza di qualsiasi tipo che una o più minacce possono sfruttare. La vulnerabilità può derivare da un'omissione o essere legata a una debolezza nei controlli in termini di rigore, completezza o coerenza e può essere di natura tecnica, procedurale, materiale, organizzativa od operativa.

Articolo 2

Oggetto e campo di applicazione

1. La presente decisione stabilisce i principi fondamentali e le norme minime di sicurezza per proteggere le ICUE.

2. La presente decisione si applica a tutti i servizi e in tutti i locali della Commissione.

3. Fatte salve indicazioni specifiche relative a particolari categorie del personale, la presente decisione si applica ai membri della Commissione, al personale della Commissione soggetto allo statuto dei funzionari dell'Unione europea e regime applicabile agli altri agenti dell'Unione, agli esperti nazionali distaccati presso la Commissione (END), ai prestatori di servizi e al loro personale, ai tirocinanti e alle persone che hanno accesso a fabbricati o altre risorse della Commissione, o alle informazioni trattate dalla Commissione.

4. Le disposizioni della presente decisione non pregiudicano la decisione 2002/47/CE, CECA, Euratom e la decisione 2004/563/CE, Euratom.

Articolo 3

Definizione delle ICUE, delle classifiche e dei contrassegni di sicurezza

1. Per «informazioni classificate UE» (ICUE) si intende qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE, la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri.

2. Le ICUE sono classificate a uno dei seguenti livelli:

a) TRES SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

b) SECRET UE/EU SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;

d) RESTREINT UE/EU RESTRICTED: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri.

3. Le ICUE recano un contrassegno di classifica di sicurezza conformemente al paragrafo 2. Esse possono recare contrassegni supplementari diversi dai contrassegni di classifica di sicurezza intesi a designare il settore di attività cui si riferiscono, identificare l'originatore, limitare la distribuzione, restringere l'uso o indicare la divulgabilità.

([1]) Regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio, del 29 febbraio 1968, che definisce lo statuto dei funzionari delle Comunità europee nonché il regime applicabile agli altri agenti di tali Comunità, ed istituisce speciali misure applicabili temporaneamente ai funzionari della Commissione (regime applicabile agli altri agenti) (GU L 56 del 4.3.1968, pag. 1).

Articolo 4

Gestione delle classifiche

1. Tutti i membri e i servizi della Commissione garantiscono che le ICUE create siano adeguatamente classificate, chiaramente identificate quali ICUE e conservino il loro livello di classifica solo per il tempo necessario.

2. Fatto salvo l'articolo 26, le ICUE non sono declassate o declassificate né i contrassegni di classifica di sicurezza di cui all'articolo 3, paragrafo 2, sono modificati o rimossi senza il previo consenso scritto dell'originatore.

3. Ove opportuno, si adottano «norme di attuazione» sul trattamento delle ICUE, compresa una guida pratica alla classificazione, a norma dell'articolo 60.

Articolo 5

Protezione di informazioni classificate

1. Le ICUE sono protette conformemente alla presente decisione e alle sue norme di attuazione.

2. Il detentore di qualsiasi ICUE è responsabile della sua protezione, a norma della presente decisione e delle relative norme di attuazione, in base alle regole stabilite al capo 4.

3. Quando gli Stati membri introducono informazioni classificate che recano un contrassegno di classifica di sicurezza nazionale nelle strutture o nelle reti della Commissione, quest'ultima protegge tali informazioni conformemente ai requisiti applicabili alle ICUE di livello equivalente come indicato nella tabella di equivalenza delle classifiche di sicurezza che figura nell'allegato I.

4. Un insieme di ICUE può richiedere un livello di protezione corrispondente a una classifica più elevata di quella dei singoli componenti.

Articolo 6

Gestione del rischio di sicurezza

1. Le misure di sicurezza per proteggere le ICUE nel corso del loro ciclo di vita sono commisurate in particolare alla rispettiva classifica di sicurezza, alla forma e al volume delle informazioni o dei materiali, all'ubicazione e alla costruzione delle strutture in cui sono conservate le ICUE e alla valutazione a livello locale della minaccia di attività dolose e/o criminali, compreso lo spionaggio, il sabotaggio e il terrorismo.

2. I piani di emergenza tengono conto della necessità di proteggere le ICUE in situazioni di emergenza onde evitare l'accesso non autorizzato, la divulgazione o la perdita di integrità o di disponibilità.

3. I piani di continuità operativa di tutti i servizi comprendono misure di prevenzione e recupero per minimizzare l'impatto di disfunzioni o incidenti gravi nel trattamento e nella conservazione delle ICUE.

Articolo 7

Attuazione della presente decisione

1. Ove opportuno, vengono adottate norme di attuazione intese a integrare o sostenere la presente decisione a norma dell'articolo 60.

2. I servizi della Commissione adottano tutte le misure necessarie che rientrano nelle loro competenze per garantire l'applicazione della presente decisione, e delle pertinenti norme di attuazione, nel trattamento o nella conservazione delle ICUE o di altre informazioni classificate.

3. Le misure di sicurezza adottate nell'attuare la presente decisione devono essere conformi ai principi per la sicurezza nella Commissione stabiliti all'articolo 3 della decisione (UE, Euratom) 2015/443.

4. Il direttore generale delle risorse umane e della sicurezza istituisce l'autorità di sicurezza della Commissione all'interno della propria direzione generale. All'autorità di sicurezza della Commissione sono assegnate le responsabilità stabilite dalla presente decisione e dalle sue norme di attuazione.

5. In tutti i servizi della Commissione, al responsabile locale della sicurezza, come stabilito all'articolo 20 della decisione (UE, Euratom) 2015/443, saranno assegnate le seguenti responsabilità generali per la protezione delle ICUE sulla base della presente decisione, in stretta collaborazione con la direzione generale Risorse umane e sicurezza:

a) gestione delle richieste di autorizzazioni di sicurezza per il personale;

b) collaborazione alle formazioni in materia di sicurezza e alle riunioni di sensibilizzazione;

c) supervisione del funzionario responsabile del controllo delle registrazioni (RCO) del servizio;

d) comunicazione delle violazioni della sicurezza e della compromissione di ICUE;

e) conservazione delle chiavi di riserva e di una traccia scritta di tutte le combinazioni;

f) assunzione di altre mansioni legate alla protezione di ICUE o stabilite dalle norme di attuazione.

Articolo 8

Violazioni della sicurezza e compromissione di ICUE

1. La violazione della sicurezza è conseguenza di un atto o omissione di una persona contrario alle norme di sicurezza contenute nella presente decisione e nelle sue norme di attuazione.

2. La compromissione di ICUE si verifica quando, in seguito a una violazione della sicurezza, le ICUE sono state diffuse in tutto o in parte a persone non autorizzate.

3. Qualsiasi violazione o sospetta violazione della sicurezza è immediatamente riferita all'autorità di sicurezza della Commissione.

4. Qualora sia noto o vi siano ragionevoli motivi di ritenere che vi sia stata compromissione o perdita di ICUE, è necessario svolgere un'indagine di sicurezza a norma dell'articolo 13 della decisione (UE, Euratom) 2015/443.

5. È necessario adottare tutte le misure necessarie a:

a) informare l'originatore;

b) assicurare che personale non direttamente interessato alla violazione indaghi sul caso per accertare i fatti;

c) valutare i potenziali danni agli interessi dell'Unione o degli Stati membri;

d) adottare i provvedimenti opportuni per impedire che i fatti si ripetano; e

e) informare le autorità competenti delle misure adottate.

6. Ogni persona responsabile di una violazione delle norme di sicurezza contenute nella presente decisione è passibile di azione disciplinare conformemente allo statuto. Ogni persona responsabile della compromissione o della perdita di ICUE è passibile di sanzioni disciplinari e/o azioni legali conformemente alle disposizioni legislative, normative e regolamentari applicabili.

CAPO 2

SICUREZZA DEL PERSONALE

Articolo 9

Definizioni

Ai fini del presente capo si intende per:

1) «autorizzazione di accesso alle ICUE», una decisione dell'autorità di sicurezza della Commissione adottata sulla base dell'assicurazione data da un'autorità competente di uno Stato membro in base alla quale un funzionario o altro agente o esperto nazionale distaccato può, quando sia stata accertata la sua necessità di conoscere e una volta istruito sulle proprie responsabilità, avere accesso alle ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore) e fino a una data stabilita; la persona che risponde a tale descrizione è indicata come in possesso del «nulla osta di sicurezza»;

2) «autorizzazione di sicurezza del personale», l'applicazione di misure volte a garantire che l'accesso alle ICUE sia consentito solo alle persone che:

   a) hanno necessità di conoscere;

   b) hanno ottenuto il nulla osta di sicurezza del livello adatto, ove opportuno; e

   c) sono state informate delle proprie responsabilità.

3) «nulla osta di sicurezza del personale» (PSC), una dichiarazione dell'autorità competente di uno Stato membro fatta al termine di un'indagine di sicurezza condotta dalle autorità competenti di uno Stato membro e attestante che una persona, quando sia stata accertata la sua necessità di conoscere e una volta istruita sulle proprie responsabilità, può avere accesso alle ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore) e a una data stabilita;

4) «certificato di nulla osta di sicurezza del personale» (PSCC), un certificato rilasciato dall'autorità competente attestante che una persona ha ottenuto il nulla osta di sicurezza o possiede un'autorizzazione di accesso alle ICUE rilasciata dall'autorità di sicurezza della Commissione in corso di validità, in cui figura il livello di ICUE cui detta persona può accedere (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), la data di validità del relativo nulla osta o autorizzazione e la data di scadenza del certificato stesso;

5) «indagine di sicurezza», le procedure investigative condotte dall'autorità competente di uno Stato membro conformemente alle disposizioni legislative e regolamentari nazionali volte ad accertare l'inesistenza di informazioni negative note sul conto di una persona che osterebbero alla concessione di un nulla osta di sicurezza fino a un livello specifico CONFIDENTIEL UE/EU CONFIDENTIAL o superiore);

Articolo 10

Principi di base

1. Una persona è autorizzata ad accedere ad ICUE dopo che:

1) sia stata accertata la sua necessità di conoscere;

2) sia stata istruita sulle norme di sicurezza per la protezione delle ICUE, nonché sulle norme e gli orientamenti di sicurezza pertinenti, ed abbia riconosciuto le proprie responsabilità in materia di protezione di tali informazioni;

3) per le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore, abbia ottenuto il nulla osta di sicurezza del livello adatto o sia in altro modo debitamente autorizzata in virtù delle proprie funzioni secondo le disposizioni legislative e regolamentari nazionali;

2. Tutte le persone le cui mansioni richiedono l'accesso a ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore dispongono del nulla osta di sicurezza del livello adatto prima di poter accedere a dette ICUE. La persona interessata esprime per iscritto il proprio consenso a essere soggetta alla procedura per il nulla osta di sicurezza del personale. In mancanza di detto consenso, alla persona non possono essere assegnati posti, funzioni o mansioni che prevedano l'accesso a informazioni classificate al livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore.

3. Le procedure per il nulla osta di sicurezza del personale sono intese a determinare se una persona, in considerazione della sua lealtà, onestà e affidabilità, può essere autorizzata ad accedere alle ICUE.

4. La lealtà, l'onestà e l'affidabilità di una persona ai fini della concessione di un nulla osta di sicurezza per l'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono accertate mediante un'indagine di sicurezza condotta dall'autorità competente di uno Stato membro conformemente alle disposizioni legislative e regolamentari nazionali.

5. L'autorità di sicurezza della Commissione è l'unica autorizzata a mantenere un collegamento con le autorità di sicurezza nazionali o altre autorità nazionali competenti per quanto riguarda tutti i nulla osta di sicurezza. Tutti i contatti tra i servizi della Commissione, il loro personale, le autorità di sicurezza nazionali e altre autorità competenti avvengono attraverso l'autorità di sicurezza della Commissione.

Articolo 11

Procedura di autorizzazione di sicurezza

1. I direttori generali o i capi servizio della Commissione individuano all'interno del proprio servizio le persone che necessitano di accedere a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore per svolgere le proprie mansioni e che pertanto necessitano di un'autorizzazione di sicurezza.

2. Non appena sia noto che una persona assumerà una posizione che necessita dell'accesso a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, il responsabile locale della sicurezza del servizio della Commissione interessato informa l'autorità di sicurezza della Commissione, che trasmette alla persona il questionario per il nulla osta di sicurezza emesso dall'autorità di sicurezza nazionale dello Stato membro con la cui nazionalità la persona è stata assunta come membro del personale delle istituzioni europee. L'interessato esprime in forma scritta il proprio consenso a essere sottoposto alla procedura per il nulla osta di sicurezza e restituisce al più presto il questionario all'autorità di sicurezza della Commissione.

3. L'autorità di sicurezza della Commissione trasmette il questionario per il nulla osta di sicurezza compilato all'autorità di sicurezza nazionale dello Stato membro con la cui nazionalità la persona è stata assunta come membro del personale delle istituzioni europee, chiedendo di avviare un'indagine di sicurezza per il livello di ICUE a cui la persona può chiedere di accedere.

4. Se viene a conoscenza di informazioni rilevanti per l'indagine di sicurezza relativa a una persona che ha chiesto un nulla osta di sicurezza, l'autorità di sicurezza della Commissione le comunica all'autorità di sicurezza nazionale competente conformemente alle pertinenti disposizioni legislative e regolamentari.

5. Al termine dell'indagine di sicurezza e non appena possibile dopo aver ricevuto la comunicazione da parte della pertinente autorità di sicurezza nazionale circa la valutazione generale dei risultati dell'indagine, l'autorità di sicurezza della Commissione:

a) può concedere un'autorizzazione per accedere alle ICUE alla persona interessata e autorizzare l'accesso alle ICUE fino al livello pertinente fino a una data specificata dalla persona ma per cinque anni al massimo, qualora dall'indagine di sicurezza emerga la garanzia dell'inesistenza di informazioni negative note che metterebbero in discussione la lealtà, l'onestà e l'affidabilità della persona;

b) se dall'indagine di sicurezza non emerge tale garanzia, conformemente alle pertinenti disposizioni legislative e regolamentari, ne dà comunicazione alla persona interessata, la quale può chiedere di essere ascoltata dall'autorità di sicurezza della Commissione, che a sua volta può rivolgersi all'autorità di sicurezza nazionale competente per ulteriori chiarimenti che quest'ultima può fornire in base alle disposizioni legislative e regolamentari nazionali. In caso di riconferma dell'esito dell'indagine di sicurezza, l'autorizzazione ad accedere alle ICUE non può essere concessa.

6. L'indagine di sicurezza e relativi risultati sono soggetti alle pertinenti disposizioni legislative e regolamentari vigenti nello Stato membro in questione, ivi comprese quelle relative ai ricorsi. Le decisioni dell'autorità di sicurezza della Commissione sono soggette a ricorso conformemente allo statuto.

7. La Commissione accetta l'autorizzazione di accesso alle ICUE rilasciata da qualsiasi altra istituzione, organo o organismo dell'Unione, purché in corso di validità. L'autorizzazione copre qualsiasi incarico della persona interessata nella Commissione. L'istituzione, l'organo o l'agenzia dell'Unione in cui persona interessata è assunta notifica all'autorità di sicurezza nazionale competente il cambiamento del datore di lavoro.

8. Se il periodo di servizio di una persona non inizia entro dodici mesi dalla comunicazione dell'esito dell'indagine di sicurezza all'autorità di sicurezza della Commissione o se vi è un'interruzione del servizio di dodici mesi, durante la quale la persona non ha occupato un posto presso la Commissione o qualunque altra istituzione, organo o agenzia dell'Unione o presso l'amministrazione di uno Stato membro, l'autorità di sicurezza della Commissione riferisce la questione all'autorità di sicurezza nazionale, affinché questa confermi se il nulla osta di sicurezza resta valido e pertinente.

9. Se viene a conoscenza di informazioni concernenti un rischio per la sicurezza posto da una persona in possesso di un'autorizzazione di sicurezza valida, l'autorità di sicurezza della Commissione le comunica all'autorità di sicurezza nazionale competente in conformità alle pertinenti disposizioni legislative e regolamentari.

10. Se un'autorità di sicurezza nazionale (NSA) comunica all'autorità di sicurezza della Commissione il ritiro della garanzia fornita conformemente al paragrafo 5, lettera a), per una persona in possesso di un'autorizzazione di accesso alle ICUE valida, l'autorità di sicurezza della Commissione può chiederle i chiarimenti che è in grado di fornire conformemente alle sue disposizioni legislative e regolamentari nazionali. Se le informazioni negative sono confermate dall'autorità di sicurezza nazionale, l'autorizzazione di sicurezza è ritirata e la persona in questione è esclusa dall'accesso alle ICUE e da posti nei quali tale accesso sia possibile o nei quali la persona potrebbe mettere a repentaglio la sicurezza.

11. La decisione di ritirare o sospendere un'autorizzazione di accesso alle ICUE ad una persona che rientra nel campo di applicazione della presente decisione e, se opportuno, i relativi motivi devono essere comunicati alla persona interessata la quale può chiedere di essere ascoltata dall'autorità di sicurezza della Commissione. Le informazioni fornite dall'NSA devono essere soggette alle pertinenti disposizioni legislative e regolamentari vigenti nello Stato membro in questione. Le decisioni adottate dall'autorità di sicurezza della Commissione in questo ambito sono soggette a ricorso conformemente allo statuto.

12. I servizi della Commissione si assicurano che gli esperti nazionali distaccati per un posto che richiede l'accesso alle ICUE presentino, prima di assumere l'incarico, un nulla osta di sicurezza del personale o un certificato di nulla osta di sicurezza del personale, conformemente alle disposizioni legislative e regolamentari nazionali, all'autorità di sicurezza della Commissione che, su tale base, rilascia un'autorizzazione di sicurezza per accedere alle ICUE fino al livello equivalente a quello indicato nel nulla osta di sicurezza nazionale, con una validità massima equivalente alla durata del loro incarico.

Accesso alle ICUE per le persone debitamente autorizzate sulla base delle loro funzioni

13. I membri della Commissione che hanno accesso alle ICUE in virtù delle proprie funzioni sulla base del trattato devono essere messi al corrente degli obblighi di sicurezza in un'ottica di tutela delle ICUE.

Registrazioni dei nulla osta e delle autorizzazioni di sicurezza

14. Le registrazioni dei nulla osta e delle autorizzazioni di sicurezza rilasciati per accedere alle ICUE devono essere conservate dall'autorità di sicurezza della Commissione a norma della presente decisione. In tali registrazioni figurano almeno il livello di ICUE cui può accedere la persona in questione, la data di concessione del nulla osta di sicurezza e il periodo di validità.

15. L'autorità di sicurezza della Commissione può rilasciare un PSCC in cui figurano il livello di ICUE cui può accedere la persona in questione (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), la data di validità della relativa autorizzazione di accesso alle ICUE e la data di scadenza del certificato stesso.

Rinnovo delle autorizzazioni di sicurezza

16. Dopo la concessione iniziale delle autorizzazioni di sicurezza e purché la persona abbia prestato servizio ininterrottamente presso la Commissione europea o altre istituzioni, organi o agenzie dell'Unione e continui ad avere bisogno di accedere alle ICUE, l'autorizzazione di sicurezza per accedere alle ICUE è riesaminata ai fini del rinnovo, di norma, ogni cinque anni dalla data di comunicazione dell'esito dell'ultima indagine di sicurezza su cui si basava.

17. L'autorità di sicurezza della Commissione può estendere la validità dell'autorizzazione di sicurezza esistente fino a dodici mesi, se non sono state ricevute informazioni negative dall'autorità di sicurezza nazionale o da un'altra autorità nazionale competente entro due mesi dalla data di trasmissione della richiesta di rinnovo e del corrispondente questionario per il nulla osta di sicurezza. Se al termine dei dodici mesi la pertinente autorità di sicurezza nazionale o un'altra autorità nazionale competente non ha comunicato il proprio parere all'autorità di sicurezza della Commissione, alla persona in questione devono essere assegnate mansioni che non necessitano di un'autorizzazione di sicurezza.

Articolo 12

Sessioni informative sull'autorizzazione di sicurezza

1. Dopo aver partecipato alle sessioni informative sull'autorizzazione di sicurezza organizzate dall'autorità di sicurezza della Commissione, tutte le persone che hanno ottenuto un'autorizzazione di sicurezza riconoscono per iscritto di aver compreso gli obblighi di protezione delle ICUE e le conseguenze che possono verificarsi se le ICUE risultano compromesse. Una registrazione di tale attestazione scritta è conservata dall'autorità di sicurezza della Commissione.

2. Tutte le persone autorizzate ad avere accesso alle ICUE o tenute a trattarle, sono sensibilizzate all'inizio e istruite periodicamente riguardo alle minacce per la sicurezza e devono comunicare immediatamente all'autorità di sicurezza della Commissione qualsiasi iniziativa o attività che ritengano sospetta o insolita.

3. Tutte le persone che cessano l'incarico per il quale era richiesto l'accesso alle ICUE sono informate dell'obbligo di continuare a proteggere le ICUE e, in caso, riconoscono per iscritto quest'obbligo.

Articolo 13

Autorizzazioni di sicurezza temporanee

1. In circostanze eccezionali, laddove sia debitamente giustificato nell'interesse del servizio e in attesa dell'esito dell'intera indagine di sicurezza, l'autorità di sicurezza della Commissione, dopo aver consultato l'autorità di sicurezza nazionale dello Stato membro di cui è cittadina la persona interessata e con riserva dell'esito dei controlli preliminari per verificare l'inesistenza di pertinenti informazioni negative note, può rilasciare un'autorizzazione temporanea per accedere alle ICUE per una funzione specifica, fatte salve le disposizioni relative al rinnovo dei nulla osta di sicurezza. Tali autorizzazioni temporanee per accedere alle ICUE sono valide per sei mesi al massimo e non danno accesso alle informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET.

2. Dopo essere state istruite in conformità all'articolo 12, paragrafo 1, tutte le persone alle quali è stata concessa un'autorizzazione temporanea riconoscono per iscritto di aver compreso gli obblighi di protezione delle ICUE e le eventuali conseguenze se le ICUE risultano compromesse. Una registrazione di tale attestazione scritta è conservata dall'autorità di sicurezza della Commissione.

Articolo 14

Partecipazione alle riunioni classificate organizzate dalla Commissione

1. I servizi della Commissione responsabili dell'organizzazione di riunioni in cui sono discusse informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, attraverso il proprio responsabile locale della sicurezza o l'organizzatore della riunione, comunicano con largo anticipo all'autorità di sicurezza della Commissione le date, gli orari, le sedi e i partecipanti di tali riunioni.

2. Fatte salve le disposizioni dell'articolo 11, paragrafo 13, le persone che devono partecipare alle riunioni organizzate dalla Commissione in cui sono discusse informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, possono farlo solo se il loro nulla osta di sicurezza o lo status del nulla osta di sicurezza è confermato. L'accesso alle riunioni classificate è negato alle persone per cui l'autorità di sicurezza della Commissione non dispone di un certificato di nulla osta di sicurezza del personale o di un'altra prova del nulla osta di sicurezza, come pure ai partecipanti della Commissione che non sono in possesso di un'autorizzazione di sicurezza.

3. Prima di organizzare una riunione classificata, l'organizzatore della riunione responsabile o il responsabile locale della sicurezza del servizio della Commissione che organizza la riunione chiede ai partecipanti esterni di presentare all'autorità di sicurezza della Commissione un certificato di nulla osta di sicurezza del personale o un'altra prova di nulla osta di sicurezza. L'autorità di sicurezza della Commissione informa il responsabile locale della sicurezza o l'organizzatore della riunione in merito al PSCC o a un'altra prova di PSC ricevuti. Se del caso, può essere usato un elenco di nomi consolidato che comprovi il nulla osta di sicurezza.

4. Qualora l'autorità di sicurezza della Commissione sia informata dalle autorità competenti che il PSC di una persona i cui compiti richiedano la partecipazione alle riunioni organizzate dalla Commissione è stato ritirato, l'autorità di sicurezza della Commissione ne informa il responsabile locale della sicurezza del servizio della Commissione che organizza la riunione.

Articolo 15

Accesso potenziale alle ICUE

Corrieri, guardie e scorte dispongono dell'autorizzazione di sicurezza di livello adatto o sono soggetti alle opportune indagini conformemente alle disposizioni legislative e regolamentari nazionali, sono informati riguardo alle procedure di sicurezza in materia di protezione delle ICUE e istruiti riguardo agli obblighi di protezione delle informazioni loro affidate.

CAPO 3

SICUREZZA MATERIALE PER LA PROTEZIONE DI INFORMAZIONI CLASSIFICATE

Articolo 16

Principi di base

1. Le misure di sicurezza materiale sono intese a impedire a intrusi l'ingresso fraudolento o con la forza, a scoraggiare, ostacolare e scoprire azioni non autorizzate e a consentire la segregazione del personale per quanto riguarda il loro accesso alle ICUE in base al principio della necessità di conoscere. Tali misure devono essere determinate in base a una procedura di gestione del rischio in conformità alla presente decisione e alle sue norme di attuazione.

2. In particolare, le misure di sicurezza materiale sono intese ad evitare l'accesso non autorizzato alle ICUE:

a) assicurando che le ICUE siano trattate e conservate in modo adeguato;

b) consentendo la segregazione del personale per quanto riguarda l'accesso alle ICUE in base alla loro necessità di conoscere e, in caso, alle loro autorizzazioni di sicurezza;

c) scoraggiando, ostacolando e scoprendo azioni non autorizzate; e

d) impedendo o ritardando l'ingresso fraudolento o con la forza di intrusi.

3. Le misure di sicurezza materiale sono attuate per tutti i locali, gli edifici, gli uffici, le stanze o altre zone in cui le ICUE sono trattate o conservate, comprese le zone che contengono i sistemi di comunicazione e informazione definiti al capo 5.

4. Le zone in cui sono conservate ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono costituite come zone protette conformemente al presente capo e approvate dall'autorità di accreditamento in materia di sicurezza della Commissione.

5. Per proteggere le ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore si usano solo attrezzature o dispositivi approvati dall'autorità di sicurezza della Commissione.

Articolo 17

Requisiti e misure di sicurezza materiale

1. Le misure di sicurezza materiale sono selezionate in base a una valutazione della minaccia effettuata dall'autorità di sicurezza della Commissione, ove opportuno consultando altri servizi della Commissione, altre istituzioni, agenzie od organi dell'Unione e/o le autorità competenti degli Stati membri. La Commissione applica una procedura di gestione del rischio per proteggere le ICUE nei propri locali al fine di garantire un livello di protezione materiale corrispondente alla valutazione del rischio. La procedura di gestione del rischio tiene conto di tutti gli elementi pertinenti, in particolare:

a) del livello di classifica delle ICUE;

b) della forma e del volume delle ICUE, tenendo conto che considerevoli quantitativi o compilazioni di ICUE possono richiedere l'applicazione di misure di protezione più rigorose;

c) dell'ambiente circostante e della struttura degli edifici o delle zone in cui sono conservate ICUE; e

d) della valutazione della minaccia rappresentata da servizi di intelligence che prendono di mira l'Unione, le sue istituzioni, organi o agenzie, o gli Stati membri e da atti di sabotaggio, terrorismo e altri atti sovversivi o criminali.

2. L'autorità di sicurezza della Commissione, nell'applicare il concetto di difesa in profondità, stabilisce l'idonea combinazione di misure di sicurezza materiale da attuare. A tale scopo, l'autorità di sicurezza della Commissione sviluppa standard, norme e criteri minimi stabiliti nelle norme di attuazione.

3. L'autorità di sicurezza della Commissione è autorizzata a effettuare ispezioni all'entrata e all'uscita come deterrente all'introduzione non autorizzata di materiale o alla sottrazione non autorizzata di ICUE da locali o edifici.

4. Quando le ICUE sono a rischio di sguardi indiscreti, anche accidentalmente, i servizi della Commissione coinvolti adottano le misure appropriate, come stabilito dall'autorità di sicurezza della Commissione, per combattere questo rischio.

5. Per le nuove strutture sono definiti requisiti di sicurezza materiale e relative specifiche funzionali di concerto con l'autorità di sicurezza della Commissione nell'ambito della pianificazione e della concezione delle strutture. Per le strutture esistenti, i requisiti di sicurezza materiale si applicano conformemente agli standard, alle norme e ai criteri minimi stabiliti nelle norme di attuazione.

Articolo 18

Attrezzature per la protezione materiale delle ICUE

1. Per la protezione materiale delle ICUE si stabiliscono due tipi di zona oggetto di protezione materiale:

a) zone amministrative; e

b) zone protette (comprese le zone protette tecnicamente).

2. L'autorità di accreditamento in materia di sicurezza della Commissione stabilisce che una zona soddisfa i requisiti per essere designata zona amministrativa, zona protetta o zona protetta tecnicamente.

3. Per le zone amministrative:

a) è stabilito un perimetro chiaramente delimitato che permette l'ispezione delle persone e, se possibile, dei veicoli;

b) l'accesso senza scorta è consentito solo alle persone debitamente autorizzate dall'autorità di sicurezza della Commissione o da un'altra autorità competente; e

c) tutte le altre persone sono scortate in ogni momento o sottoposte a controlli equivalenti.

4. Per le zone protette:

a) è stabilito un perimetro chiaramente delimitato e protetto attraverso cui sono controllati tutti gli ingressi e le uscite per mezzo di un lasciapassare o di un sistema di riconoscimento personale;

b) l'accesso senza scorta è consentito solo alle persone in possesso di un nulla osta di sicurezza ed espressamente autorizzate a entrare nella zona in base alla loro necessità di conoscere;

c) tutte le altre persone sono scortate in ogni momento o sottoposte a controlli equivalenti.

5. Se l'ingresso in una zona protetta costituisce, a tutti i fini pratici, un accesso diretto alle informazioni classificate ivi conservate, si applicano i seguenti requisiti supplementari:

a) il livello più elevato di classifica di sicurezza delle informazioni normalmente conservate nella zona è chiaramente indicato;

b) tutti i visitatori richiedono un'autorizzazione specifica ad entrare nella zona, sono scortati in ogni momento e sono in possesso del nulla osta di sicurezza adatto, a meno che non siano presi provvedimenti intesi a garantire che non sia possibile alcun accesso alle ICUE.

6. Le zone protette che vengono protette dall'ascolto indiscreto sono designate zone protette tecnicamente. Si applicano i seguenti requisiti supplementari:

a) tali zone sono dotate di sistemi di rilevamento delle intrusioni (IDS), chiuse a chiave se non occupate e sorvegliate se occupate. Le chiavi sono gestite conformemente all'articolo 20;

b) tutte le persone o tutto il materiale che accedono a tali zone sono soggetti a controllo;

c) tali zone sono regolarmente soggette a ispezioni materiali e/o tecniche da parte dell'autorità di sicurezza della Commissione. Dette ispezioni sono inoltre effettuate dopo qualsiasi ingresso non autorizzato, effettivo o sospettato; e

d) tali zone sono prive di linee di comunicazione, telefoni o altri dispositivi di comunicazione ed attrezzature elettriche o elettroniche non autorizzati.

7. Nonostante il paragrafo 6, lettera d), prima di essere usati in zone in cui si svolgono riunioni o attività che implicano informazioni classificate di livello SECRET UE/EU SECRET o superiore, e laddove la minaccia alle ICUE sia valutata alta, tutti i dispositivi di comunicazione e tutte le attrezzature elettriche o elettroniche sono preventivamente esaminati dall'autorità di sicurezza della Commissione al fine di garantire che nessuna informazione intelligibile sia trasmessa inavvertitamente o illegalmente da tali attrezzature all'esterno del perimetro della zona protetta.

8. Ove opportuno, le zone protette non occupate da personale in servizio 24 ore su 24 sono ispezionate al termine del normale orario di lavoro e a intervalli casuali al di fuori del normale orario di lavoro, tranne nel caso in cui vi sia installato un IDS.

9. Le zone protette e le zone protette tecnicamente possono essere istituite in via temporanea in una zona amministrativa per una riunione classificata o per altri motivi analoghi.

10. Il responsabile locale della sicurezza del servizio della Commissione interessato elabora procedure operative di sicurezza per tutte le aree protette di cui è responsabile che stabiliscono, conformemente alle disposizioni della presente decisione e delle sue norme di attuazione:

a) il livello delle ICUE che possono essere trattate e conservate nella zona;

b) le misure di sorveglianza e di protezione che devono essere applicate;

c) le persone autorizzate ad accedere senza scorta alla zona in virtù della loro necessità di conoscere e della loro autorizzazione di sicurezza;

d) ove opportuno, le procedure relative alle scorte o alla protezione delle ICUE quando si autorizza l'accesso di altre persone alla zona;

e) ogni altra misura e procedura pertinente.

11. Nelle zone protette sono costruite camere blindate. Le pareti, il pavimento, il soffitto, le finestre e le porte provviste di serratura sono approvati dall'autorità di sicurezza della Commissione e offrono una protezione equivalente a quella di un contenitore di sicurezza approvato per la conservazione di ICUE dello stesso livello di classifica.

Articolo 19

Misure di protezione materiale per il trattamento e la conservazione delle ICUE

1. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED possono essere trattate:

a) in una zona protetta;

b) in una zona amministrativa purché le ICUE siano protette dall'accesso di persone non autorizzate;

c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore trasporti le ICUE conformemente all'articolo 31, e si sia impegnato ad osservare le misure compensative stabilite nelle norme di attuazione per garantire che le ICUE siano protette dall'accesso di persone non autorizzate.

2. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED sono conservate in idonei mobili da ufficio chiusi a chiave, in una zona amministrativa o in una zona protetta. Esse possono essere temporaneamente conservate all'esterno di una zona protetta o di una zona amministrativa purché il detentore si sia impegnato ad osservare le misure compensative stabilite nelle norme di attuazione.

3. Le ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET possono essere trattate:

a) in una zona protetta;

b) in una zona amministrativa purché le ICUE siano protette dall'accesso di persone non autorizzate; o

c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore:

   i) si sia impegnato ad osservare le misure compensative stabilite nelle norme di attuazione per garantire che le ICUE siano protette dall'accesso di persone non autorizzate;

   ii) tenga le ICUE sempre sotto il proprio controllo; e

   iii) in caso di documenti cartacei, ne abbia informato il competente ufficio di registrazione.

4. Le ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET sono conservate in una zona protetta in un contenitore di sicurezza o in una camera blindata.

5. Le ICUE classificate di livello TRÈS SECRET UE/EU TOP SECRET sono trattate in una zona protetta, istituita e mantenuta dall'autorità di sicurezza della Commissione, e accreditate a tale livello dall'autorità di accreditamento in materia di sicurezza della Commissione.

6. Le ICUE classificate di livello TRÈS SECRET UE/EU TOP SECRET sono conservate in una zona protetta, accreditate a tale livello dall'autorità di accreditamento in materia di sicurezza della Commissione, secondo uno delle modalità seguenti:

a) in un contenitore di sicurezza conformemente alle disposizioni dell'articolo 18, con almeno uno dei seguenti controlli supplementari:

   (1) protezione continua o verifica da parte di personale con nulla osta di sicurezza o personale di servizio;

   (2) un IDS approvato, in combinazione con personale di sicurezza incaricato degli interventi;

   o

b) in una camera blindata dotata di IDS, in combinazione con personale di sicurezza incaricato degli interventi.

Articolo 20

Controllo delle chiavi e delle combinazioni usate per proteggere le ICUE

1. Le procedure di gestione delle chiavi e delle combinazioni per gli uffici, le stanze, le camere blindate e i contenitori di sicurezza devono essere stabilite nelle norme di attuazione in base all'articolo 60. Tali procedure hanno lo scopo di proteggere dall'accesso non autorizzato.

2. Le combinazioni sono conosciute a memoria dal minor numero possibile di persone che hanno necessità di conoscerle. Le combinazioni dei contenitori di sicurezza e delle camere blindate in cui sono conservate ICUE sono modificate:

a) al ricevimento di ogni nuovo contenitore;

b) in caso di sostituzione del personale che conosce la combinazione;

c) in caso di effettiva o sospetta compromissione;

d) se una serratura è stata oggetto di manutenzione o riparazione; e

e) almeno ogni dodici mesi.

CAPO 4

GESTIONE DELLE INFORMAZIONI CLASSIFICATE DELL'UE

Articolo 21

Principi di base

1. Tutti i documenti ICUE devono essere gestiti conformemente alla politica di gestione dei documenti della Commissione e di conseguenza registrati, archiviati, conservati e infine eliminati, sottoposti a campionamento o trasferiti agli archivi storici in base all'elenco comune di conservazione a livello della Commissione per i fascicoli dell'Unione europea.

2. Le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono registrate a fini di sicurezza prima della diffusione e all'atto della ricezione. Le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET sono registrate in uffici di registrazione dedicati.

3. Alla Commissione è istituito un sistema di registrazione dell'ICUE conformemente alle disposizioni dell'articolo 27.

4. I servizi e i locali in cui sono trattate o conservate ICUE sono sottoposti a ispezioni periodiche da parte dell'autorità di sicurezza della Commissione.

5. Le ICUE sono veicolate tra i servizi e i locali al di fuori delle zone oggetto di protezione materiale secondo le modalità seguenti:

a) di norma, le ICUE sono trasmesse con mezzi elettronici protetti mediante prodotti crittografici approvati conformemente al capo 5;

b) qualora non siano usati i mezzi di cui alla lettera a), le ICUE sono trasportate:

   i) su supporti elettronici (ad esempio chiave USB, CD, disco rigido) protetti mediante prodotti crittografici approvati conformemente al capo 5; o

   ii) in tutti gli altri casi, come stabilito nelle norme di attuazione.

Articolo 22

Classifiche e contrassegni

1. Le informazioni sono classificate quando devono essere protette con riferimento alla loro riservatezza conformemente all'articolo 3, paragrafo 1.

2. L'originatore delle ICUE è incaricato di determinare il livello di classifica di sicurezza, conformemente alle norme di attuazione, alle norme e agli orientamenti in materia di classifica, e della diffusione iniziale delle informazioni.

3. Il livello di classifica dell'ICUE è stabilito conformemente all'articolo 3, paragrafo 2, e alle pertinenti norme di attuazione.

4. La classifica di sicurezza è chiaramente e correttamente indicata, indipendentemente dal fatto che le ICUE siano in forma cartacea, orale, elettronica o in altra forma.

5. Le singole parti di un determinato documento (ad esempio pagine, paragrafi, sezioni, annessi, appendici, allegati e materiale accluso) possono richiedere classifiche differenti e sono contraddistinte di conseguenza anche nel caso in cui siano conservate in forma elettronica.

6. Il livello generale di classifica di un documento o file è almeno quello del suo componente con livello di classifica più elevato. Quando si riprendono informazioni da varie fonti, il prodotto finale è riesaminato per determinarne il livello generale di classifica di sicurezza, in quanto può richiedere una classifica più elevata di quella dei suoi componenti.

7. Per quanto possibile, i documenti che contengono parti con livelli di classifica diversi sono impostati in modo che le parti con un livello di classifica diverso possano essere facilmente individuate e, se necessario, separate.

8. La classifica di una lettera o di una nota che comprende materiale accluso corrisponde a quello dell'elemento accluso con livello di classifica più elevato. L'originatore indica chiaramente il livello di classifica della lettera o della nota quando è separata dal materiale accluso mediante un contrassegno adeguato, ad esempio:

CONFIDENTIEL UE/EU CONFIDENTIAL

Senza allegato/i RESTREINT UE/EU RESTRICTED

Articolo 23

Contrassegni

Oltre a uno dei contrassegni di classifica di sicurezza di cui all'articolo 3, paragrafo 2, le ICUE possono recare altri contrassegni quali:

a) un identificatore per designare l'originatore;

b) avvertenze, parole chiave o acronimi per specificare il settore di attività cui si riferisce il documento, una distribuzione particolare sulla base del principio della necessità di conoscere o restrizioni d'uso;

c) contrassegni di divulgabilità;

d) se del caso, la data o un evento specifico a seguito dei quali possono essere declassate o declassificate.

Articolo 24

Contrassegni di classifica abbreviati

1. Contrassegni di classifica abbreviati standard possono essere usati per indicare il livello di classifica di singoli paragrafi di un testo. Le abbreviazioni non sostituiscono i contrassegni di classifica per esteso.

2. Le seguenti abbreviazioni standard possono essere usate nei documenti classificati UE per indicare il livello di classifica di sezioni o parti del testo di dimensioni inferiori a una pagina:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Articolo 25

Creazione di ICUE

1. Quando si produce un documento classificato UE:

a) ciascuna pagina è contrassegnata chiaramente con il livello di classifica;

b) ciascuna pagina è numerata;

c) il documento reca un numero di riferimento e un oggetto che non è in sé un'informazione classificata, a meno che non sia contrassegnato come tale;

d) il documento è datato;

e) i documenti classificati di livello SECRET UE/EU SECRET o superiore, se devono essere distribuiti in più copie, recano un numero di copia sul ciascuna pagina.

2. Qualora non sia possibile applicare il paragrafo 1 alle ICUE, sono adottate altre misure appropriate conformemente alle norme di attuazione.

Articolo 26

Declassamento e declassificazione delle ICUE

1. Al momento della creazione delle ICUE l'originatore indica, laddove possibile, se possono essere declassate o declassificate ad una certa data o in seguito ad un dato evento.

2. I servizi della Commissione riesaminano periodicamente le ICUE di cui sono originatori per accertare che il livello di classifica sia ancora applicabile. Le norme di attuazione stabiliscono un sistema per riesaminare almeno ogni cinque anni il livello di classifica delle ICUE registrate delle quali la Commissione è l'originatore. Tale riesame non è necessario se l'originatore ha indicato fin dall'inizio che le informazioni saranno automaticamente declassate o declassificate e se le informazioni sono state contrassegnate di conseguenza.

3. Le informazioni classificate di livello RESTREINT UE/EU RESTRICTED di cui la Commissione è l'originatore saranno considerate automaticamente declassificate dopo trent'anni, conformemente al regolamento (CEE, Euratom) n. 354/83 modificato dal regolamento (CE, Euratom) n. 1700/2003 del Consiglio ([1]).

Articolo 27

Sistema di registrazione delle ICUE in Commissione

1. Fatto salvo l'articolo 52, paragrafo 5, in tutti i servizi della Commissione in cui sono trattate o conservate ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET occorre identificare un ufficio di registrazione locale delle ICUE per assicurarne un trattamento conforme alla presente decisione.

2. L'ufficio di registrazione delle ICUE gestito dal segretariato generale è l'ufficio centrale di registrazione delle ICUE della Commissione. Esso funge da:

— ufficio di registrazione locale delle ICUE per il segretariato generale della Commissione,

— ufficio di registrazione delle ICUE per gli uffici privati dei membri della Commissione, a meno che essi non dispongano di ufficio locale di registrazione delle ICUE specifico,

— ufficio di registrazione delle ICUE per le direzioni generali o i servizi che non dispongono di un ufficio di registrazione locale delle ICUE,

— principale punto d'ingresso e uscita per tutti gli scambi di informazioni classificate di livello RESTREINT UE/EU RESTRICTED e superiore fino al livello SECRET UE/EU SECRET tra la Commissione e i propri servizi e gli Stati terzi e le organizzazioni internazionali e, se previsto in base ad accordi specifici, per altre istituzioni, agenzie e organi dell'Unione.

3. Alla Commissione l'autorità di sicurezza della Commissione designa un ufficio di registrazione che funge da autorità centrale ricevente e trasmittente delle informazioni classificate TRÈS SECRET UE/EU TOP SECRET. Per il trattamento di tali informazioni a fini di registrazione possono essere designati, se necessario, uffici dipendenti.

4. Gli uffici dipendenti non possono trasmettere documenti di livello TRÈS SECRET UE/EU TOP SECRET direttamente ad altri uffici dipendenti dello stesso ufficio centrale di registrazione TRÈS SECRET UE/EU TOP SECRET o all'esterno senza l'esplicito accordo di quest'ultimo.

5. Gli uffici di registrazione sono costituiti in zone protette, come stabilito al capo 3, e accreditati dall'autorità di accreditamento in materia di sicurezza della Commissione.

Articolo 28

Funzionario responsabile del controllo delle registrazioni

1. Tutti gli uffici di registrazione delle ICUE sono gestiti da un funzionario responsabile del controllo delle registrazioni (RCO).

2. L'RCO deve essere munito di apposito nulla osta di sicurezza.

3. L'RCO è soggetto alla supervisione del responsabile locale della sicurezza del servizio della Commissione per quanto attiene all'applicazione delle disposizioni sul trattamento delle ICUE e al rispetto delle pertinenti misure, norme e orientamenti di sicurezza.

4. Nell'ambito delle proprie responsabilità di gestione dell'ufficio di registrazione delle ICUE cui è stato assegnato, all'RCO saranno assegnate le seguenti responsabilità generali conformemente alla presente decisione e alle norme di attuazione, standard e orientamenti corrispondenti:

— gestire le operazioni relative alla registrazione, conservazione, riproduzione, traduzione, trasmissione, spedizione e distruzione o trasferimento al servizio dell'archivio storico delle ICUE,

— verificare periodicamente la necessità di mantenere la classificazione delle informazioni,

— assumere altre mansioni legate alla protezione delle ICUE stabilite nelle norme di attuazione.

Articolo 29

Registrazione di ICUE a fini di sicurezza

1. Ai fini della presente decisione, per registrazione a fini di sicurezza («registrazione») si intende l'applicazione di procedure che registrano il ciclo di vita delle ICUE, compresa la diffusione.

([1]) Regolamento (CE, Euratom) n. 1700/2003 del Consiglio del 22 settembre 2003 che modifica il regolamento (CEE, Euratom) n. 354/83 che rende accessibili al pubblico gli archivi storici della Comunità economica europea e della Comunità europea dell'energia atomica (GU L 243 del 27.9.2003, pag. 1).

2. Le informazioni o i materiali classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore sono registrati in uffici di registrazione dedicati quando entrano o lasciano un'entità organizzativa.

3. Quando l'ICUE è trattata o conservata mediante un sistema di comunicazione e informazione (CIS), le procedure di registrazione possono essere eseguite mediante procedure interne allo stesso CIS.

4. Disposizioni più dettagliate relative alla registrazione delle ICUE a fini di sicurezza figureranno nelle norme di attuazione.

Articolo 30

Riproduzione e traduzione di documenti classificati UE

1. I documenti di livello TRÈS SECRET UE/EU TOP SECRET possono essere riprodotti o tradotti solo previo consenso scritto dell'originatore.

2. Se l'originatore di documenti classificati di livello SECRET UE/EU SECRET o inferiore non ha imposto limitazioni alla riproduzione o alla traduzione, detti documenti possono essere riprodotti o tradotti su istruzione del detentore.

3. Le misure di sicurezza applicabili al documento originale si applicano alle copie e alle traduzioni.

Articolo 31

Trasporto delle ICUE

1. Le ICUE sono trasportate in modo da proteggerle da divulgazione non autorizzata durante il trasporto.

2. Il trasporto di ICUE è soggetto a misure di protezione che sono:

— commisurate al livello di classifica delle ICUE trasportate, e

— adattate alle condizioni specifiche di trasporto, in particolare se le ICUE sono trasportate:

  — all'interno di un edificio della Commissione o di un gruppo autonomo di edifici della Commissione,

  — tra edifici della Commissione situati nello stesso Stato membro,

  — all'interno dell'Unione,

  — dall'Unione al territorio di uno Stato terzo, e

  — adeguate alla natura e alla forma delle ICUE.

3. Le misure di protezione sono specificate nelle norme di attuazione o, nel caso di progetti e programmi di cui all'articolo 42, sono parte integrante delle pertinenti istruzioni di sicurezza del programma/progetto (PSI).

4. Le norme di attuazione o le PSI comprendono disposizioni commisurate al livello delle ICUE, in merito:

— al tipo di trasporto, vale a dire il trasporto a mano, il trasporto tramite valigia diplomatica o corriere militare, il trasporto mediante servizi postali o servizi di corriere commerciale,

— al confezionamento delle ICUE,

— alle contromisure tecniche per le ICUE trasportate con mezzi elettronici,

— ad altre misure procedurali, fisiche o elettroniche,

— alle procedure di registrazione,

— al ricorso a personale di sicurezza autorizzato.

5. Se le ICUE sono trasportate con mezzi elettronici, e in deroga all'articolo 21, paragrafo 5, le misure di protezione stabilite nelle pertinenti norme di attuazione possono essere integrate da opportune contromisure tecniche prescritte dall'autorità di sicurezza della Commissione per minimizzare il rischio di perdita o di compromissione.

Articolo 32

Distruzione di ICUE

1. I documenti classificati UE che non sono più necessari possono essere distrutti, tenendo conto dei regolamenti in materia di archiviazione e delle norme e dei regolamenti della Commissione sulla gestione e l'archiviazione dei documenti, in particolare l'elenco comune di conservazione a livello della Commissione.

2. Le ICUE di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore sono distrutte dall'RCO dell'ufficio di registrazione delle ICUE competente su istruzione del detentore o di un'autorità competente. L'RCO aggiorna di conseguenza i repertori e gli altri dati relativi alla registrazione.

3. Per i documenti classificati SECRET UE/EU SECRET o TRÈS SECRET UE/EU TOP SECRET effettua la distruzione in presenza di un testimone che possiede un nulla osta di sicurezza almeno fino al livello di classifica del documento da distruggere.

4. L'ufficiale del registro e il testimone, laddove sia richiesta la presenza di quest'ultimo, firmano un certificato di distruzione che è archiviato presso l'ufficio di registrazione. L'RCO dell'ufficio di registrazione competente conserva i certificati di distruzione dei documenti TRÈS SECRET UE/EU TOP SECRET per un periodo di almeno dieci anni e quelli dei documenti CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET per un periodo di almeno cinque anni.

5. I documenti classificati, compresi quelli di livello RESTREINT UE/EU RESTRICTED, sono distrutti con metodi definiti nelle norme di attuazione e conformi alle pertinenti norme dell'UE o equivalenti.

6. I supporti informatici delle ICUE sono distrutti in conformità alle procedure stabilite nelle norme di attuazione.

Articolo 33

Distruzione delle ICUE in casi di emergenza

1. I servizi della Commissione che dispongono di ICUE predispongono piani, in base alle condizioni vigenti in loco, per la protezione del materiale classificato UE in situazioni di crisi, compresa, se necessaria, la distruzione di emergenza e piani di evacuazione. Essi emanano le istruzioni che ritengono necessarie per impedire che le ICUE cadano nelle mani di persone non autorizzate.

2. Le disposizioni per la protezione e/o la distruzione di materiale CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET in situazioni di crisi non compromette in alcun modo la protezione o la distruzione di materiale TRÈS SECRET UE/EU TOP SECRET, ivi compresa l'attrezzatura di cifratura, il cui trattamento è prioritario rispetto a tutte le altre funzioni.

3. In caso di emergenza, se c'è un rischio imminente di divulgazione non autorizzata, le ICUE sono distrutte dal detentore in modo tale da non poter essere ricostruite né totalmente né parzialmente. L'originatore e l'ufficio di registrazione d'origine sono informati della distruzione d'emergenza delle ICUE registrate.

4. Disposizioni più dettagliate relative alla distruzione delle ICUE figureranno nelle norme di attuazione

CAPO 5

PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE UE NEI SISTEMI DI COMUNICAZIONE E INFORMAZIONE (CIS)

Articolo 34

Principi fondamentali della garanzia di sicurezza delle informazioni

1. Per «garanzia di sicurezza delle informazioni (IA) nel campo dei sistemi di comunicazione e informazione» si intende la fiducia nel fatto che tali sistemi proteggeranno le informazioni che trattano e funzioneranno nel modo dovuto e a tempo debito sotto il controllo degli utenti legittimi.

2. Un'efficace garanzia di sicurezza delle informazioni assicura livelli adeguati di:

— autenticità: garanzia che l'informazione è veritiera e proviene da fonti in buona fede,

— disponibilità: proprietà di accessibilità e utilizzabilità su richiesta di un'entità autorizzata,

— riservatezza: proprietà per cui l'informazione non è divulgata a persone, entità o procedure non autorizzate,

— integrità: proprietà di tutela della precisione e della completezza delle informazioni e delle risorse,

— non disconoscibilità: capacità di provare che un'azione o un evento sono effettivamente accaduti e non possono essere negati in seguito.

3. L'IA si basa su una procedura di gestione del rischio.

Articolo 35

Definizioni

Ai fini del presente capo si intende per:

a) «accreditamento», l'autorizzazione e l'approvazione formale accordata a un sistema di comunicazione e informazione dall'autorità di accreditamento in materia di sicurezza (SAA) per il trattamento di ICUE nel suo contesto operativo, in seguito alla convalida formale del piano di sicurezza e alla sua corretta attuazione;

b) «procedura di accreditamento», le misure e i compiti necessari richiesti dall'autorità di accreditamento in materia di sicurezza prima di accordare l'accreditamento. Tali misure e compiti sono specificati in una norma di procedura di accreditamento;

c) «sistema di comunicazione e informazione (CIS)», ogni sistema che consente il trattamento delle informazioni in forma elettronica. Un sistema di comunicazione e informazione comprende l'insieme delle risorse necessarie al suo funzionamento, ivi compresi l'infrastruttura, l'organizzazione, il personale e le risorse dell'informazione;

d) «rischio residuo», il rischio che permane una volta attuate delle misure di sicurezza, dato che non tutte le minacce possono essere neutralizzate né tutte le vulnerabilità eliminate;

e) «rischio», la possibilità che una data minaccia sfrutti le vulnerabilità interne ed esterne di un'organizzazione o di uno qualsiasi dei sistemi da essa utilizzati, arrecando pertanto danno all'organizzazione o ai suoi beni materiali o immateriali. È calcolato come una combinazione tra le probabilità del verificarsi delle minacce e il loro impatto;

f) «accettazione del rischio», la decisione di accettare la permanenza di un rischio residuo in seguito al trattamento del rischio;

g) «valutazione del rischio», l'identificazione delle minacce e delle vulnerabilità e l'esecuzione delle relative analisi del rischio, ossia l'analisi della probabilità e dell'impatto;

h) «comunicazione del rischio», lo sviluppo della sensibilizzazione ai rischi tra le comunità di utenti del CIS, informando di tali rischi le autorità di approvazione e riferendo sugli stessi alle autorità operative;

i) «trattamento del rischio», mitigazione, rimozione, riduzione (tramite un'opportuna combinazione di misure tecniche, materiali, organizzative o procedurali), trasferimento o controllo del rischio.

Articolo 36

CIS che trattano ICUE

1. I CIS trattano le ICUE conformemente al concetto di IA.

2. Per i CIS che trattano ICUE, la conformità alla politica della Commissione in materia di sicurezza dei sistemi di informazione, di cui alla decisione C(2006) 3602 ([1]) della Commissione, implica quanto segue:

a) per attuare la politica in materia di sicurezza dei sistemi di informazione si applica l'approccio basato sul ciclo di Deming (ciclo Plan-Do-Check-Act) durante l'intero ciclo di vita del sistema di informazioni;

b) le esigenze in materia di sicurezza devono essere identificate attraverso una valutazione d'impatto;

c) il sistema di informazione e i dati al suo interno devono essere oggetto di una classificazione formale delle attività;

([1]) Decisione C(2006) 3602, del 16 agosto 2006, sulle norme relative alla sicurezza dei sistemi di informazione utilizzati dalla Commissione europea.

d) devono essere attuate tutte le misure di sicurezza obbligatorie stabilite dalla politica in materia di sicurezza dei sistemi di informazione;

e) deve essere applicata una procedura di gestione del rischio, che comprende le seguenti fasi: identificazione della minaccia e della vulnerabilità, valutazione del rischio, trattamento del rischio, accettazione del rischio e comunicazione del rischio;

f) è definito, attuato, verificato e riesaminato un piano di sicurezza, che comprende la politica di sicurezza e le procedure operative di sicurezza.

3. Tutto il personale coinvolto nella progettazione, nello sviluppo, nel collaudo, nel funzionamento, nella gestione o nell'utilizzo di CIS che trattano ICUE notifica all'autorità di accreditamento in materia di sicurezza ogni potenziale lacuna di sicurezza, incidente, violazione o compromissione della sicurezza che potrebbe avere conseguenze sulla protezione del CIS e/o delle ICUE in esso contenute.

4. Qualora la protezione delle ICUE sia assicurata mediante prodotti crittografici, tali prodotti sono approvati secondo le modalità seguenti:

a) di preferenza la scelta va ai prodotti che sono stati approvati dal Consiglio o dal segretario generale del Consiglio nel suo ruolo di autorità di approvazione degli apparati crittografici del Consiglio, su raccomandazione del gruppo di esperti in materia di sicurezza della Commissione;

b) ove giustificato da specifici motivi operativi, l'autorità di approvazione degli apparati crittografici (CAA) può, su raccomandazione del gruppo di esperti in materia di sicurezza della Commissione, derogare ai requisiti di cui al punto a) e rilasciare un'approvazione temporanea per un periodo specifico.

5. Durante la trasmissione, il trattamento e l'archiviazione di ICUE con mezzi elettronici si usano prodotti crittografici approvati. In deroga a tale requisito, in situazioni di emergenza o in configurazioni tecniche specifiche si possono applicare procedure specifiche previa approvazione della CAA.

6. Sono attuate misure di sicurezza per proteggere i CIS che trattano informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore in modo tale che tali informazioni non possano essere compromesse da radiazioni elettromagnetiche non intenzionali («misure di sicurezza TEMPEST»). Dette misure di sicurezza sono commisurate al rischio di sfruttamento e al livello di classifica delle informazioni.

7. All'autorità di sicurezza della Commissione sono assegnate le seguenti funzioni:

— autorità IA (IAA),

— autorità di accreditamento di sicurezza (SAA),

— autorità TEMPEST (TA),

— autorità di approvazione degli apparati crittografici (CAA),

— autorità di distribuzione degli apparati crittografici (CDA).

8. L'autorità di sicurezza della Commissione nomina l'autorità operativa IA per ciascun sistema.

9. Le responsabilità delle funzioni descritte nei paragrafi 7 e 8 saranno definite nelle norme di attuazione.

Articolo 37

Accreditamento di CIS che trattano ICUE

1. Tutti i CIS che trattano ICUE sono soggetti a una procedura di accreditamento basata sui principi dell'IA, il cui livello di dettaglio deve essere commisurato al livello di protezione richiesto.

2. La procedura di accreditamento comprende la convalida formale, da parte dell'SAA della Commissione, del piano di sicurezza per il CIS pertinente al fine di garantire che:

a) la procedura di gestione del rischio, di cui all'articolo 36, paragrafo 2, sia stata effettuata in modo adeguato;

b) il proprietario del sistema abbia accettato consapevolmente il rischio residuo; e

c) sia stato raggiunto un livello sufficiente di protezione del CIS, e delle ICUE in esso trattate, conformemente alla presente decisione.

3. L'SAA della Commissione rilascia una dichiarazione di accreditamento che determina il livello di classifica più elevato delle ICUE che può essere trattato nel CIS nonché i termini e le condizioni associati al funzionamento. Ciò non pregiudica i compiti affidati al comitato di accreditamento di sicurezza stabiliti all'articolo 11 del regolamento (UE) n. 512/2014 del Parlamento europeo e del Consiglio ([1]).

4. Un comitato di accreditamento di sicurezza (SAB) comune è responsabile dell'accreditamento dei CIS della Commissione che coinvolgono diverse parti. Esso è composto di un rappresentante SAA di ciascuna parte coinvolta e vi partecipa un rappresentante SAA della Commissione.

5. La procedura di accreditamento consiste in una serie di compiti assegnati alle parti coinvolte. Il proprietario del sistema CIS è il solo responsabile della preparazione dei fascicoli e della documentazione.

6. L'accreditamento compete all'SAA della Commissione, che, in qualsiasi momento del ciclo di vita del CIS, ha diritto di:

a) chiedere l'applicazione di una procedura di accreditamento;

b) effettuare audit o ispezioni del CIS;

c) qualora non siano più soddisfatte le condizioni di funzionamento, chiedere la definizione e l'attuazione effettiva di un piano di miglioramento della sicurezza entro tempi ben definiti, arrivando a ritirare l'autorizzazione al funzionamento del CIS fino a quando le condizioni di funzionamento non siano nuovamente soddisfatte.

7. La procedura di accreditamento è stabilita in una norma sulla procedura di accreditamento per i CIS che trattano ICUE, che è adottata a norma dell'articolo 10, paragrafo 3, della decisione C(2006) 3602.

Articolo 38

Situazioni di emergenza

1. In deroga alle disposizioni del presente capo, le procedure specifiche descritte di seguito possono essere applicate in casi di emergenza, come in situazioni di crisi, conflitti, guerre imminenti o già in corso o in circostanze operative eccezionali.

2. Le ICUE possono essere trasmesse, previo consenso dell'autorità competente, usando prodotti crittografici approvati per un livello di classifica inferiore o senza cifratura nel caso in cui un ritardo causerebbe un danno manifestamente maggiore di quello dovuto all'eventuale divulgazione del materiale classificato e se:

a) il mittente e il destinatario non hanno l'attrezzatura di cifratura necessaria; e

b) il materiale classificato non può essere trasmesso in tempo utile con altri mezzi.

3. Le informazioni classificate trasmesse nelle circostanze di cui al paragrafo 1 non recano alcun contrassegno o indicazione che le distinguano da informazioni non classificate o che possono essere protette mediante prodotti crittografici disponibili. I destinatari sono informati tempestivamente, con altri mezzi, del livello di classifica.

4. È presentato un successivo rapporto all'autorità competente e al gruppo di esperti in materia di sicurezza della Commissione.

CAPO 6

SICUREZZA INDUSTRIALE

Articolo 39

Principi di base

1. Per «sicurezza industriale» si intende l'applicazione di misure che assicurino la protezione delle ICUE:

a) nell'ambito di contratti classificati, da parte di:

   i) candidati od offerenti attraverso la procedura di appalto e aggiudicazione;

   ii) contraenti o subcontraenti lungo tutto il ciclo di vita dei contratti classificati;

([1]) Regolamento (UE) n. 512/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, che modifica il regolamento (UE) n. 912/2010 che istituisce l'Agenzia del GNSS europeo (GU L 150 del 20.5.2014, pag. 72).

b) nell'ambito di convenzioni di sovvenzione classificate, da parte di:

i) i richiedenti durante le procedure di concessione di una sovvenzione;

ii) i beneficiari lungo tutto il ciclo di vita delle convenzioni di sovvenzione classificate.

2. Tali contratti o convenzioni di sovvenzione non contemplano le informazioni classificate di livello TRÈS SECRET UE/EU TOP SECRET.

3. Se non stabilito diversamente, le disposizioni del presente capo relative ai contratti o ai contraenti si applicano anche ai subcontratti o ai subcontraenti classificati.

Articolo 40

Definizioni

Ai fini del presente capo si intende per:

a) «contratto classificato», un contratto quadro o un contratto, conformemente al regolamento (CE, Euratom) n. 1605/2002 del Consiglio ([1]), stipulato dalla Commissione o da uno dei suoi servizi, con un contraente per la fornitura di beni mobili o immobili, l'esecuzione di lavori o la prestazione di servizi, la cui esecuzione richiede o implica la creazione, il trattamento o la conservazione di ICUE;

b) «subcontratto classificato», un contratto stipulato da un contraente della Commissione o uno dei suoi servizi con un altro contraente (vale a dire il subcontraente) per la fornitura di beni mobili o immobili, l'esecuzione di lavori o la prestazione di servizi, la cui esecuzione richiede o implica la creazione, il trattamento o la conservazione di ICUE;

c) «convenzione di sovvenzione classificata», una convenzione con cui la Commissione concede una sovvenzione, come stabilito nella parte I, titolo VI, del regolamento (CE, Euratom) n. 1605/2002, la cui esecuzione richiede o implica la creazione, il trattamento o la conservazione di ICUE;

d) «autorità di sicurezza designata» (DSA), l'autorità che fa capo all'autorità di sicurezza nazionale (NSA) di uno Stato membro, incaricata di comunicare ai soggetti industriali o di altra natura la linea politica nazionale riguardo a tutti gli aspetti della sicurezza industriale e di fornire guida e assistenza nell'attuazione della medesima. La funzione della DSA può essere espletata dall'NSA o da qualsiasi altra autorità competente.

Articolo 41

Procedura per contratti classificati o convenzioni di sovvenzione

1. In quanto autorità contraente, ogni servizio della Commissione, nell'aggiudicare un contratto classificato o una convezione di sovvenzione, assicura che le norme minime sulla sicurezza industriale previste nel presente capo siano menzionate o integrate nel contratto e che siano rispettate.

2. Ai fini del paragrafo 1, i servizi competenti della Commissione chiedono il parere della direzione generale Risorse umane e sicurezza, in particolare della direzione Sicurezza, e si assicurano che i modelli di contratti, subcontratti e convenzioni di sovvenzione includano disposizioni che riflettano i principi di base e le norme minime per proteggere le ICUE che devono essere rispettate sia dai contraenti e subcontraenti, sia dai beneficiari delle convenzioni di sovvenzione.

3. La Commissione collabora strettamente con l'NSA, la DSA o altra autorità competente degli Stati membri interessati.

4. L'autorità contraente che intende lanciare una procedura intesa a concludere un contratto classificato o una convenzione di sovvenzione chiede il parere dell'autorità di sicurezza della Commissione sulle questioni relative alla natura e agli elementi classificati della procedura durante tutte le sue fasi.

5. I modelli dei contratti e dei subcontratti classificati, delle convenzioni di sovvenzione classificate, delle comunicazioni contrattuali, degli orientamenti sulle circostanze in cui sono richiesti i nulla osta di sicurezza delle imprese (FSC), le istruzioni di sicurezza del programma o progetto (PSI), le lettere sugli aspetti di sicurezza (SAL), le visite, la trasmissione e il trasporto di ICUE nell'ambito di contratti o convenzioni di sovvenzione classificati sono definiti nelle norme di attuazione sulla sicurezza industriale, previa consultazione del gruppo di esperti in materia di sicurezza della Commissione.

([1]) Regolamento (CE, Euratom) n. 1605/2002 del Consiglio, 25 giugno 2002, che stabilisce il regolamento finanziario applicabile al bilancio generale delle Comunità europee (GU L 248 del 16.9.2002, pag. 1).

6. La Commissione può concludere contratti o convenzioni di sovvenzione classificati che comportano o implicano l'accesso a, il trattamento o la conservazione di ICUE da parte di operatori economici registrati in uno Stato membro o in uno Stato terzo che abbia concluso un accordo o un accordo amministrativo conformemente al capo 7 della presente decisione.

Articolo 42

Elementi di sicurezza in un contratto classificato o in una convenzione di sovvenzione

1. I contratti classificati o le convenzioni di sovvenzione comprendono i seguenti elementi di sicurezza:

istruzione di sicurezza del programma o progetto:

a) per «istruzione di sicurezza del programma o progetto» (PSI) si intende un elenco delle procedure di sicurezza che sono applicate a un programma o progetto specifico per uniformare le procedure di sicurezza. L'elenco può essere riveduto per tutta la durata del programma o progetto;

b) la direzione generale Risorse umane e sicurezza sviluppa una PSI generica. I servizi della Commissione responsabili dei programmi o dei progetti che prevedono il trattamento o la conservazione di ICUE possono sviluppare, ove opportuno, PSI specifiche basate sulla PSI generica;

c) una PSI specifica è sviluppata in particolare per i programmi e i progetti caratterizzati da portata, entità o complessità considerevoli o dalla molteplicità e/o la diversità dei contraenti, dei beneficiari nonché degli altri partner e portatori d'interessi coinvolti, ad esempio per quanto riguarda il loro status giuridico. La PSI specifica è sviluppata dai servizi della Commissione che gestiscono il programma o progetto, in stretta collaborazione con la direzione generale Risorse umane e sicurezza;

d) la direzione generale Risorse umane e sicurezza chiede un parere sulle PSI generiche e specifiche al gruppo di esperti in materia di sicurezza della Commissione;

lettera sugli aspetti di sicurezza (SAL):

a) per «lettera sugli aspetti di sicurezza» (SAL) si intende un pacchetto di condizioni contrattuali specifiche emesso dall'autorità contraente, che è parte integrante di un contratto classificato implicante l'accesso o la creazione di ICUE e in cui sono individuati i requisiti di sicurezza e gli elementi del contratto che richiedono una protezione di sicurezza;

b) i requisiti di sicurezza specifici del contratto sono indicati in una SAL. Ove opportuno, tale SAL contiene la guida alle classifiche di sicurezza (SCG) ed è parte integrante di un contratto o subcontratto classificato o di una convenzione di sovvenzione;

c) la SAL contiene le disposizioni che impongono al contraente o al beneficiario di osservare le norme minime stabilite dalla presente decisione. L'autorità contraente assicura che la SAL indichi che l'inosservanza di tali norme minime può essere motivo sufficiente di estinzione del contratto o della convenzione di sovvenzione.

2. Sia le PSI che le SAL comprendono una guida alle classifiche di sicurezza, quale elemento di sicurezza obbligatorio:

a) per «guida alle classifiche di sicurezza» (SCG), si intende un documento che illustra gli elementi di un programma, progetto, contratto o convenzione di sovvenzione classificati e precisa i livelli di classifica di sicurezza applicabili. L'SCG può essere integrata per tutta la durata del programma, progetto, contratto o convenzione di sovvenzione e gli elementi informativi possono essere riclassificati o declassati; se esistente, l'SCG fa parte della SAL;

b) prima di indire un bando di gara o di concludere un contratto classificato, il servizio della Commissione in quanto autorità contraente stabilisce la classifica di sicurezza delle informazioni che devono essere fornite ai candidati, agli offerenti o ai contraenti, nonché la classifica di sicurezza delle informazioni che il contraente deve creare. A tale scopo elabora un'SCG ai fini dell'esecuzione del contratto conformemente alla presente decisione e alle sue norme di attuazione, previa consultazione dell'autorità di sicurezza della Commissione.

c) Per stabilire la classifica di sicurezza dei vari elementi di un contratto classificato si applicano i principi seguenti:

i) nel redigere la SCG, il servizio della Commissione, in quanto autorità contraente, tiene conto di tutti gli aspetti di sicurezza, tra cui la classifica di sicurezza assegnata all'informazione fornita e approvata che l'originatore dell'informazione deve usare per il contratto;

ii) il livello generale di classifica del contratto non può essere inferiore alla classifica più elevata di uno dei suoi elementi; e

iii) ove opportuno, l'autorità contraente si mette in contatto, attraverso l'autorità di sicurezza della Commissione, con le NSA, DSA degli Stati membri o altre autorità di sicurezza competenti interessate in caso di qualsiasi modifica nella classifica delle informazioni create dai contraenti o ad essi fornite nell'esecuzione di un contratto e di eventuali ulteriori modifiche alla SCG.

Articolo 43

Accesso del personale dei contraenti e dei beneficiari alle ICUE

L'autorità contraente o che eroga la sovvenzione assicura che il contratto classificato o la convenzione di sovvenzione classificata prevedano disposizioni che consentono al personale di un contraente, subcontraente o beneficiario che ne abbiano bisogno per l'esecuzione del contratto, subcontratto o convenzione di sovvenzione classificati, l'accesso alle ICUE solo se il personale:

a) dispone dell'autorizzazione di sicurezza del livello pertinente o è autorizzato debitamente in altro modo da una necessità di conoscere riconosciuta;

b) sia stato istruito sulle norme di sicurezza applicabili per la protezione delle ICUE ed abbia riconosciuto le proprie responsabilità in materia di protezione di tali informazioni;

c) abbia ricevuto il nulla osta di sicurezza al livello pertinente per le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET dalle rispettive NSA e DSA o da altre autorità competenti.

Articolo 44

Nulla osta di sicurezza delle imprese

1. Per «nulla osta di sicurezza delle imprese» (FSC) si intende una decisione amministrativa di un'NSA, una DSA o altra autorità di sicurezza competente, secondo la quale un'impresa è in grado, sotto il profilo della sicurezza, di offrire un adeguato livello di protezione alle ICUE ad un determinato livello di classifica di sicurezza;

2. L'FSC concesso dall'NSA/DSA o altra autorità di sicurezza competente di uno Stato membro per indicare, conformemente alle disposizioni legislative e regolamentari nazionali, che un operatore economico è in grado di proteggere le ICUE al livello adatto di classifica (CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET) all'interno delle proprie strutture, viene presentata all'autorità di sicurezza della Commissione, che la trasmette al servizio della Commissione operante in quanto autorità contraente o che eroga la sovvenzione, prima che a un candidato, offerente o contraente oppure a un richiedente o beneficiario della sovvenzione siano comunicate delle ICUE o possa essere concesso l'accesso a tali informazioni classificate.

3. Ove opportuno, attraverso l'autorità di sicurezza della Commissione, l'autorità contraente notifica all'NSA, DSA pertinente o altra autorità di sicurezza competente che è necessario un FSC per l'esecuzione del contratto. È richiesto un FSC o un PSC laddove occorre fornire ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante il processo di presentazione delle offerte.

4. L'autorità contraente o che eroga la sovvenzione non assegna all'offerente o partecipante selezionato un contratto classificato o una convenzione di sovvenzione prima di aver ricevuto conferma dall'NSA, DSA, o da altra autorità di sicurezza competente dello Stato membro in cui ha sede il contraente o subcontraente interessato, che laddove necessario è stato rilasciato l'FSC adatto.

5. Se l'NSA, DSA o altra autorità di sicurezza competente che ha rilasciato un FSC notifica l'autorità di sicurezza della Commissione in merito a modifiche dell'FSC, quest'ultima le comunica al servizio della Commissione operante come autorità contraente o che eroga la sovvenzione. In caso di subcontratto, l'NSA, DSA o altra autorità di sicurezza competente è informata di conseguenza.

6. La revoca dell'FSC da parte dell'NSA/DSA interessata o da altra autorità di sicurezza competente è motivo sufficiente per far sì che l'autorità contraente o che eroga la sovvenzione estingua il contratto classificato o escluda un candidato, offerente o richiedente dalla gara. Nei modelli di contratto e di convenzione di sovvenzione che saranno elaborati occorre inserire una disposizione a tale scopo

Articolo 45

Disposizioni per contratti e convenzioni di sovvenzione classificati

1. Qualora a un candidato, offerente o richiedente siano fornite ICUE durante la procedura di aggiudicazione, l'invito a presentare offerte contiene una disposizione che impone al candidato, offerente o richiedente che non ha presentato un'offerta o proposta o che non è stato selezionato l'obbligo di restituire tutti i documenti classificati entro un periodo di tempo determinato.

2. L'autorità contraente o che eroga la sovvenzione notifica, attraverso l'autorità di sicurezza della Commissione, all'NSA, DSA competente o altra autorità di sicurezza competente l'aggiudicazione di un contratto o di una convenzione di sovvenzione classificati e i dati pertinenti, quali il nome del/i contraente/i o beneficiari, la durata del contratto e il livello massimo di classifica.

3. In caso di estinzione di detti contratti o convenzioni di sovvenzione, l'autorità contraente o che eroga la sovvenzione ne notifica immediatamente, attraverso l'autorità di sicurezza della Commissione, l'NSA, DSA o altra autorità di sicurezza competente dello Stato membro in cui il contraente o beneficiario della sovvenzione ha sede.

4. Di norma, alla cessazione del contratto o della convenzione di sovvenzione classificati oppure al termine della partecipazione di un beneficiario della sovvenzione, il contraente o il beneficiario della sovvenzione è tenuto a restituire all'autorità contraente o che eroga la sovvenzione le ICUE in suo possesso.

5. La SAL contiene disposizioni specifiche per l'eliminazione delle ICUE durante l'esecuzione o alla cessazione del contratto o della convenzione di sovvenzione classificati.

6. Se è autorizzato a conservare le ICUE alla cessazione di un contratto o una convenzione di sovvenzione classificati, il contraente o beneficiario della sovvenzione continua a rispettare le norme minime previste dalla presente decisione nonché a proteggere la riservatezza delle ICUE.

Articolo 46

Disposizioni specifiche per i contratti classificati

1. Le condizioni pertinenti alla protezione delle ICUE alle quali è ammesso il subcontratto da parte del contraente sono definite nel bando di gara e nel contratto classificato.

2. Prima di subappaltare parti di un contratto classificato il contraente ottiene il consenso dell'autorità contraente. Nessun subcontratto che prevede l'accesso a ICUE può essere aggiudicato a subcontraenti con sede in paesi terzi, a meno che vi sia un quadro normativo per la sicurezza delle informazioni come previsto al capo 7.

3. Spetta al contraente assicurare che tutte le attività del subcontratto si svolgano secondo le norme minime previste dalla presente decisione e astenersi dal fornire ICUE a un subcontraente senza previo consenso scritto dell'autorità contraente.

4. Per quanto riguarda le ICUE create o trattate dal contraente, la Commissione è considerata l'originatore e i diritti spettanti all'originatore sono esercitati dall'autorità contraente.

Articolo 47

Visite relative a contratti classificati

1. Se un membro del personale della Commissione, dei contraenti o dei beneficiari della sovvenzione richiede l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei rispettivi locali per l'esecuzione di un contratto o di una convenzione di sovvenzione classificati, le visite sono fissate di concerto con le NSA, DSA o altre autorità di sicurezza competenti interessate. L'autorità di sicurezza della Commissione è informata di tali visite. Tuttavia, nel contesto di programmi o progetti specifici, le NSA, DSA o altre autorità di sicurezza competenti possono anche convenire una procedura in base alla quale tali visite possono essere fissate direttamente.

2. Tutti i visitatori dispongono di un nulla osta di sicurezza adatto e hanno una necessità di conoscere per accedere alle ICUE relative al contratto classificato.

3. I visitatori possono accedere solo alle ICUE relative all'oggetto della visita.

4. disposizioni più dettagliate figureranno nelle norme di attuazione.

5. Il rispetto delle disposizioni in merito alle visite relative ai contratti classificati, stabilite nella presente decisione e nelle norme di attuazione di cui al paragrafo 4, è obbligatorio.

Articolo 48

Trasmissione e trasporto di ICUE in relazione ai contratti o alle convenzioni di sovvenzione classificati

1. Per la trasmissione di ICUE mediante mezzi elettronici si applicano le pertinenti disposizioni del capo 5 della presente decisione.

2. Per quanto riguarda il trasporto di ICUE, si applicano le pertinenti disposizioni del capo 4 della presente decisione e delle relative norme di attuazione, conformemente alle disposizioni legislative e regolamentari nazionali.

3. Per il trasporto di materiale classificato come merce, nel fissare i dispositivi di sicurezza si applicano i principi seguenti:

a) la sicurezza è garantita in tutte le fasi del trasporto dal luogo di origine alla destinazione finale;

b) il livello di protezione attribuito a una spedizione è determinato dal livello di classifica più elevato del materiale trasportato;

c) qualsiasi movimento transfrontaliero di materiale classificato CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET è subordinato a un programma di trasporto elaborato dal mittente e approvato dalle NSA, DSA o altra autorità di sicurezza competente interessata;

d) i tragitti sono effettuati, per quanto possibile, da punto a punto e sono completati quanto più rapidamente possibile secondo le circostanze;

e) gli itinerari dovrebbero attraversare, per quanto possibile, unicamente Stati membri. Gli itinerari attraverso Stati diversi dagli Stati membri dovrebbero essere seguiti solo se autorizzati dall'NSA/DSA o da altra autorità di sicurezza competente degli Stati di spedizione e di destinazione.

Articolo 49

Trasmissione di ICUE a contraenti o beneficiari di sovvenzioni situati in Stati terzi

Le ICUE sono trasmesse a contraenti o beneficiari della sovvenzione situati in Stati terzi secondo misure di sicurezza convenute tra l'autorità di sicurezza della Commissione, il servizio della Commissione in quanto autorità contraente o che eroga la sovvenzione e l'NSA, DSA o altra autorità di sicurezza competente del paese terzo interessato in cui il contraente o il beneficiario della sovvenzione ha sede.

Articolo 50

Trattamento di informazioni classificate RESTREINT UE/EU RESTRICTED nell'ambito di contratti o convenzioni di sovvenzione classificati

1. La protezione delle informazioni classificate RESTREINT UE/EU RESTRICTED trattate o conservate nell'ambito di contratti o convenzioni di sovvenzione classificati si basa su principi di proporzionalità e efficienza economica.

2. Non sono richiesti FSC o PSC nell'ambito di contratti o convenzioni di sovvenzione classificati che implicano il trattamento di informazioni classificate di livello RESTREINT UE/EU RESTRICTED.

3. Se un contratto o una convenzione di sovvenzione comportano il trattamento di informazioni classificate RESTREINT UE/EU RESTRICTED in un CIS gestito da un contraente o beneficiario di sovvenzione, l'autorità contraente o che eroga la sovvenzione garantisce, previa consultazione dell'autorità di sicurezza della Commissione, che nel contratto o convenzione di sovvenzione siano specificati i requisiti tecnici e amministrativi necessari in merito all'accreditamento o all'approvazione del CIS commisurati al rischio valutato, tenendo conto di tutti i fattori pertinenti. La portata dell'accreditamento o dell'approvazione di tale CIS è concordata tra l'autorità di sicurezza della Commissione e l'NSA, DSA competente.

CAPO 7

SCAMBIO DI INFORMAZIONI CLASSIFICATE CON ALTRE ISTITUZIONI, AGENZIE, ORGANI E UFFICI DELL'UNIONE, CON GLI STATI MEMBRI E CON STATI TERZI E ORGANIZZAZIONI INTERNAZIONALI

Articolo 51

Principi di base

1. Se la Commissione o uno dei suoi servizi stabilisce che è necessario scambiare ICUE con un'altra istituzione, agenzia, organo o ufficio dell'Unione o con uno Stato terzo od organizzazione internazionale, vengono adottate le misure necessarie per predisporre un adeguato quadro giuridico o amministrativo a tale scopo, che potrebbe comprendere accordi sulla sicurezza delle informazioni o accordi amministrativi conclusi a norma dei pertinenti regolamenti.

2. Fatto salvo l'articolo 57, le ICUE sono scambiate con un'altra istituzione, agenzia, organo o ufficio dell'Unione o con uno Stato terzo o un'organizzazione internazionale solo se è predisposto il suddetto quadro giuridico o amministrativo adeguato e se vi sono garanzie sufficienti in merito all'applicazione di principi di base e norme minime equivalenti per la protezione di informazioni classificate da parte dell'istituzione, agenzia, organo o ufficio dell'Unione o dello Stato terzo o dell'organizzazione internazionale interessati.

Articolo 52

Scambio di ICUE con altre istituzioni, agenzie, organi e uffici dell'Unione

1. Prima di stipulare un accordo amministrativo per lo scambio di ICUE con altre istituzioni, agenzie, organi o uffici dell'Unione, la Commissione si assicura che l'istituzione, l'agenzia, l'organo o l'ufficio dell'Unione interessati:

a) disponga di un quadro normativo per la protezione delle ICUE che preveda principi di base e norme minime equivalenti a quelli stabiliti nella presente decisione e nelle relative norme di attuazione;

b) applichi norme di sicurezza e orientamenti in materia di sicurezza del personale, sicurezza materiale, gestione delle ICUE e sicurezza dei sistemi di informazione e comunicazione (CIS) che garantiscano un livello di protezione delle ICUE equivalente a quello della Commissione;

c) contrassegni come ICUE le informazioni classificate prodotte.

2. La direzione generale Risorse umane e sicurezza, in stretta collaborazione con altri pertinenti servizi della Commissione, è il servizio capofila della Commissione per la conclusione di accordi amministrativi per lo scambio di ICUE con altre istituzioni, agenzie, organi o uffici dell'Unione.

3. Di norma gli accordi amministrativi assumono la forma di uno scambio di lettere firmate dal direttore generale delle risorse umane e sicurezza a nome della Commissione.

4. Prima di stipulare un accordo amministrativo sullo scambio di ICUE, l'autorità di sicurezza della Commissione effettua una visita per valutare il quadro normativo che tutela le ICUE e accertare l'efficacia delle misure attuate per proteggere le ICUE. Gli accordi amministrativi entrano in vigore e le ICUE sono scambiate solo se il risultato della visita di valutazione è soddisfacente e sono state rispettate le raccomandazioni formulate in tale occasione. Sono effettuate regolari visite di valutazione per verificare il rispetto degli accordi amministrativi e l'attuazione delle misure di sicurezza nel continuo rispetto dei principi di base e delle norme minime concordati.

5. Nella Commissione, l'ufficio di registrazione delle ICUE gestito dal Segretariato generale è di norma il principale punto d'ingresso e uscita per gli scambi delle informazioni classificate con altre istituzioni, agenzie, organi e uffici dell'Unione. Tuttavia, se per motivi operativi, organizzativi o di sicurezza è più appropriato per la protezione delle ICUE, gli uffici locali di registrazione delle ICUE istituiti nei servizi della Commissione conformemente alla presente decisione operano come principale punto d'ingresso e uscita delle informazioni classificate, nell'ambito delle competenze dei servizi della Commissione interessati.

6. Il gruppo di esperti in materia di sicurezza della Commissione è informato delle procedure per la conclusione di accordi amministrativi a norma del paragrafo 2.

Articolo 53

Scambio di ICUE con gli Stati membri

1. Le ICUE possono essere scambiate con gli Stati membri e comunicate ad essi a patto che essi proteggano tali informazioni in base ai requisiti applicabili alle informazioni classificate che recano un contrassegno di classifica di sicurezza nazionale di livello equivalente, come indicato nella tabella di equivalenza delle classifiche di sicurezza contenuta nell'allegato I.

2. Quando gli Stati membri introducono informazioni classificate che recano un contrassegno di classifica di sicurezza nazionale nelle strutture o nelle reti dell'Unione europea, quest'ultima protegge tali informazioni conformemente ai requisiti applicabili alle ICUE di livello equivalente come indicato nella tabella di equivalenza delle classifiche di sicurezza che figura nell'allegato I.

Articolo 54

Scambio di ICUE con Stati terzi e organizzazioni internazionali

1. Se la Commissione stabilisce di avere necessità a lungo termine di scambiare informazioni classificate con Stati terzi od organizzazioni internazionali, vengono adottate le misure necessarie per predisporre un adeguato quadro giuridico o amministrativo a tale scopo, che potrebbe comprendere accordi sulla sicurezza delle informazioni o accordi amministrativi conclusi a norma dei pertinenti regolamenti.

2. Gli accordi sulla sicurezza delle informazioni o gli accordi amministrativi di cui al paragrafo 1 contengono disposizioni intese ad assicurare che gli Stati terzi o le organizzazioni internazionali che ricevono le ICUE conferiscano loro una protezione appropriata al loro livello di classifica e conforme a norme minime che equivalgono a quelle previste nella presente decisione.

3. La Commissione può pattuire accordi amministrativi a norma dell'articolo 56, se la classifica delle ICUE non supera in genere il livello RESTREINT UE/EU RESTRICTED.

4. Gli accordi amministrativi per lo scambio di informazioni classificate di cui al paragrafo 3 contengono disposizioni intese ad assicurare che gli Stati terzi o le organizzazioni internazionali che ricevono le ICUE conferiscano loro una protezione appropriata al loro livello di classifica e conforme a norme minime che equivalgono a quelle previste nella presente decisione. Il gruppo di esperti in materia di sicurezza della Commissione è consultato in merito alla conclusione di accordi sulla sicurezza delle informazioni o di accordi amministrativi.

5. La decisione di comunicare a Stati terzi od organizzazioni internazionali le ICUE originate dalla Commissione è presa caso per caso dal servizio della Commissione all'origine di dette ICUE nella Commissione, in funzione della natura e del contenuto di tali informazioni, della necessità di conoscere del destinatario e dell'entità dei vantaggi per l'Unione. Se l'originatore delle informazioni classificate che si desiderano comunicare, o delle fonti che può contenere, non è la Commissione, il servizio della Commissione che detiene tali informazioni classificate chiede anzitutto il consenso scritto dell'originatore. Se non è possibile stabilire l'originatore, il servizio della Commissione che detiene tali informazioni classificate ne assume la responsabilità dopo aver consultato il gruppo di esperti in materia di sicurezza della Commissione.

Articolo 55

Accordi sulla sicurezza delle informazioni

1. Gli accordi sulla sicurezza delle informazioni con Stati terzi od organizzazioni internazionali sono conclusi a norma dell'articolo 218 del TFUE.

2. Gli accordi sulla sicurezza delle informazioni:

a) stabiliscono i principi fondamentali e le norme minime che disciplinano lo scambio di informazioni classificate tra l'Unione e uno Stato terzo od organizzazione internazionale;

b) prevedono modalità tecniche di attuazione da concordare tra le competenti autorità di sicurezza delle istituzioni e degli organi pertinenti dell'Unione e la competente autorità di sicurezza dello Stato terzo o dell'organizzazione internazionale interessati. Tali accordi tengono conto del livello di protezione garantito dalle normative, dalle strutture e dalle procedure in materia di sicurezza esistenti nello Stato terzo o nell'organizzazione internazionale in questione;

c) prevedono che, prima dello scambio di informazioni classificate nel quadro dell'accordo, si accerti che il destinatario è in grado di proteggere e salvaguardare in modo appropriato le informazioni classificate che gli vengono fornite.

3. Qualora a norma dell'articolo 51, paragrafo 1, si stabilisca la necessità di scambiare informazioni classificate, la Commissione consulta il Servizio europeo per l'azione esterna, il Segretariato generale del Consiglio e altre istituzioni e organi dell'Unione, se opportuno, per decidere se occorre presentare una raccomandazione a norma dell'articolo 218, paragrafo 3, del TFUE.

4. Le ICUE non sono oggetto di scambio per via elettronica, a meno che non sia esplicitamente previsto dall'accordo sulla sicurezza delle informazioni o dalle modalità tecniche di attuazione.

5. Nella Commissione, l'ufficio di registrazione delle ICUE gestito dal segretariato generale è di norma il principale punto d'ingresso e uscita per gli scambi delle informazioni classificate con Stati terzi e organizzazioni internazionali. Tuttavia, se per motivi operativi, organizzativi o di sicurezza è più appropriato per la protezione delle ICUE, gli uffici locali di registrazione delle ICUE istituiti nei servizi della Commissione conformemente alla presente decisione operano come principale punto d'ingresso e uscita delle informazioni classificate, nell'ambito delle competenze dei servizi della Commissione interessati.

6. Per valutare l'efficacia delle normative, delle strutture e delle procedure di sicurezza nello Stato terzo o nell'organizzazione internazionale in questione, la Commissione, in collaborazione con altre istituzioni, agenzie o organi dell'Unione, partecipa a visite di valutazione di comune accordo con lo Stato terzo o l'organizzazione internazionale interessati. Tali visite valutano:

a) il quadro normativo applicabile per la protezione delle informazioni classificate;

b) eventuali aspetti specifici della politica di sicurezza e del modo in cui è organizzata la sicurezza nello Stato terzo o nell'organizzazione internazionale che potrebbero avere un impatto sul livello delle informazioni classificate che possono essere oggetto di scambio;

c) le misure e le procedure di sicurezza effettivamente attuate; e

d) le procedure per il nulla osta di sicurezza per il livello delle ICUE da comunicare.

Articolo 56

Disposizioni amministrative

1. Qualora nell'ambito di un contesto politico o giuridico dell'Unione sussista una necessità a lungo termine di scambiare informazioni classificate in generale di livello non superiore a RESTREINT UE/EU RESTRICTED con uno Stato terzo o un'organizzazione internazionale e qualora l'autorità di sicurezza della Commissione, previa consultazione del gruppo di esperti in materia di sicurezza della Commissione, abbia stabilito in particolare che la parte in questione non possiede un sistema di sicurezza sufficientemente sviluppato da consentirle di concludere un accordo sulla sicurezza delle informazioni, la Commissione può pattuire accordi amministrativi con le autorità competenti dello Stato terzo o dell'organizzazione internazionale in questione.

2. Gli accordi amministrativi assumono di norma la forma di uno scambio di lettere.

3. Prima di concludere l'accordo viene effettuata una visita di valutazione. Il gruppo di esperti in materia di sicurezza della Commissione è informato dei risultati della visita di valutazione. Qualora vi siano ragioni eccezionali per uno scambio urgente di informazioni classificate, possono essere comunicate ICUE purché venga compiuto ogni sforzo per effettuare tale visita di valutazione il più presto possibile.

4. Le ICUE non sono oggetto di scambio per via elettronica a meno che non sia esplicitamente previsto dall'accordo amministrativo.

Articolo 57

Comunicazione eccezionale ad hoc di ICUE

1. Se non sono stati conclusi accordi sulla sicurezza delle informazioni o accordi amministrativi e se la Commissione o uno dei suoi servizi stabilisce che sussista una necessità eccezionale, nell'ambito di un contesto politico o giuridico dell'Unione, di comunicare ICUE ad uno Stato terzo od ad un'organizzazione internazionale, l'autorità di sicurezza della Commissione, per quanto possibile, verifica con le autorità di sicurezza dello Stato terzo o dell'organizzazione internazionale interessati che le rispettive normative, strutture e procedure in materia di sicurezza siano tali da garantire che le ICUE comunicate siano protette secondo norme non meno rigorose di quelle previste nella presente decisione.

2. La decisione di comunicare ICUE allo Stato terzo o all'organizzazione internazionale in questione, previa consultazione del gruppo di esperti in materia di sicurezza della Commissione, viene presa dalla Commissione in base a una proposta del membro della Commissione responsabile della sicurezza.

3. In seguito alla decisione della Commissione di comunicare ICUE e previo consenso scritto dell'originatore, compresi gli originatori delle fonti che possono contenere, il servizio competente della Commissione inoltra le informazioni in questione, che riportano un contrassegno di divulgabilità indicante lo Stato terzo o l'organizzazione internazionale cui sono state comunicate. Prima o al momento della comunicazione effettiva, il terzo in questione si impegna per iscritto a proteggere le ICUE che riceve conformemente ai principi fondamentali e alle norme minime stabiliti nella presente decisione.

CAPO 8

DISPOSIZIONI FINALI

Articolo 58

Sostituzione di precedenti decisioni

La presente decisione abroga e sostituisce la decisione 2001/844/CE, CECA, Euratom della Commissione ([1]).

Articolo 59

Informazioni classificate create prima dell'entrata in vigore della presente decisione

1. Tutte le ICUE classificate conformemente alla decisione 2001/844/CE, CECA, Euratom continuano a essere protette conformemente alle pertinenti disposizioni della presente decisione.

2. Tutte le informazioni classificate in possesso della Commissione alla data di entrata in vigore della decisione 2001/844/CE, CECA, Euratom, eccetto le informazioni classificate Euratom:

a) se create dalla Commissione, continuano a essere considerate riclassificate per difetto al livello «RISERVATO UE», a meno che l'autore abbia deciso di conferire loro un'altra classificazione entro il 31 gennaio 2002 e ne abbia informato tutti i destinatari del documento in questione;

b) se create da fonti esterne alla Commissione, conservano la classificazione originaria e sono quindi trattate come ICUE di grado equivalente, a meno che l'autore acconsenta a declassificarle o declassarle.

Articolo 60

Norme di attuazione e comunicazioni di sicurezza

1. Se necessario, l'adozione delle norme di attuazione della presente decisione sarà oggetto di una decisione separata della Commissione volta ad abilitare il membro della Commissione responsabile della sicurezza, nel pieno rispetto del regolamento interno.

2. Una volta abilitato in forza della suddetta decisione della Commissione, il membro della Commissione responsabile della sicurezza può elaborare comunicazioni di sicurezza che definiscano orientamenti e migliori pratiche in materia nel quadro della presente decisione e delle relative norme di attuazione.

3. La Commissione può delegare i compiti di cui ai paragrafi 1 e 2 al direttore generale delle risorse umane e della sicurezza con decisione di delega separata, nel pieno rispetto del regolamento interno.

Articolo 61

Entrata in vigore

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

Fatto a Bruxelles, il 13 marzo 2015

Per la Commissione

Il presidente

Jean-Claude JUNCKER

([1]) Decisione 2001/844/CE, CECA, Euratom della Commissione, del 29 novembre 2001, che modifica il regolamento interno della Commissione (GU L 317 del 3.12.2001, pag. 1).

ALLEGATO I

EQUIVALENZA DELLE CLASSIFICHE DI SICUREZZA

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgio	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota [1] in calce
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Repubblica ceca	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danimarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	STRENG GEHEIM	GEHEIM	VS [2] — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlanda	Top Secret	Secret	Confidential	Restricted
Grecia	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spagna	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francia	Très Secret Défense	Secret Défense	Confidentiel Défense	nota [3] in calce
Croazia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Cipro	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettonia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Lussemburgo	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Ungheria	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Paesi Bassi	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polonia	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portogallo	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovacchia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Svezia (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Regno Unito	UK TOP SECRET	UK SECRET	Senza equivalente (5)	UK OFFICIAL — SENSITIVE

(1) Diffusion Restreinte/Beperkte Verspreiding non è una classifica di sicurezza in Belgio. Il Belgio tratta e protegge le informazioni «RESTREINT UE/EU RESTRICTED» in modo non meno rigoroso delle norme e procedure descritte nella normativa di sicurezza del Consiglio dell'Unione europea.

(2) Germania: VS = Verschlusssache (informazioni classificate).

(3) La Francia non usa il grado di classifica «RESTREINT» nel suo sistema nazionale. La Francia tratta e protegge le informazioni «RESTREINT UE/EU RESTRICTED» in modo non meno rigoroso delle norme e procedure descritte nella normativa di sicurezza del Consiglio dell'Unione europea.

(4) Svezia: i contrassegni di classifica di sicurezza della riga superiore sono usati dalle autorità della difesa e i contrassegni della riga inferiore sono usati dalle altre autorità.

(5) Il Regno Unito tratta e protegge le ICUE contrassegnate «CONFIDENTIEL UE/EU CONFIDENTIAL» in conformità ai requisiti protettivi di sicurezza per «UK SECRET».

ALLEGATO II

ELENCO DELLE ABBREVIAZIONI

Acronimo	Significato
CA	Autorità degli apparati crittografici
CAA	Autorità di approvazione degli apparati crittografici
CCTV	Televisione a circuito chiuso (Closed Circuit Television)
CDA	Autorità di distribuzione degli apparati crittografici
CIS	Sistemi di comunicazione e informazione che trattano ICUE
DSA	autorità di sicurezza designata (Designated Security Authority)
ICUE	Informazioni classificate UE
FSC	Nulla osta di sicurezza dei luoghi (Facility Security Clearance)
IA	Garanzia di sicurezza delle informazioni
IAA	Autorità per la garanzia di sicurezza delle informazioni
IDS	Sistema di rilevamento delle intrusioni (Intrusion Detection System)
IT/TI	Tecnologia dell'informazione
LSO	Responsabile locale della sicurezza (Local Security Officer)
NSA	Autorità nazionale di sicurezza (National Security Authority)
PSC	Nulla osta di sicurezza del personale (Personnel Security Clearance)
PSCC	Certificato di nulla osta di sicurezza del personale (Personnel Security Clearance Certificate)
PSI	Istruzioni di sicurezza del programma/progetto (Programme/Project Security Instructions)
RCO	Funzionario responsabile del controllo delle registrazioni (Registry Control Officer)
SAA	Autorità di accreditamento di sicurezza
SAL	Lettera sugli aspetti di sicurezza (Security Aspects Letter)
SCG	Guida alle classifiche di sicurezza (Security Classification Guide)
SecOPs	Procedure operative di sicurezza (Security Operating Procedures)
TA	Autorità TEMPEST
TFUE	Trattato sul funzionamento dell'Unione europea

ALLEGATO III

ELENCO DELLE AUTORITÀ DI SICUREZZA NAZIONALE

BELGIO

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

BULGARIA

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

REPUBBLICA CECA

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

DANIMARCA

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

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

GERMANIA

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

ESTONIA

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

GRECIA

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

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

SPAGNA

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

FRANCIA

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 171758177
Fax + 33 171758200

CROAZIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tel. +385 14681222
Fax + 385 14686049
Website: www.uvns.hr

IRLANDA

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

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

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

LETTONIA

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

LITUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUSSEMBURGO

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

UNGHERIA

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Fax +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

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

PAESI BASSI

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

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

AUSTRIA

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

POLONIA

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2 A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTOGALLO

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

ROMANIA

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

SLOVENIA

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

SLOVACCHIA

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

FINLANDIA

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

SVEZIA

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

REGNO UNITO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk