Gazzetta ufficiale dell'Unione europea

L 72

Edizione in lingua italiana

Legislazione

58° anno

17 marzo 2015

Sommario

IT

Gli atti i cui titoli sono stampati in caratteri chiari appartengono alla gestione corrente. Essi sono adottati nel quadro della politica agricola e hanno generalmente una durata di validità limitata.

I titoli degli altri atti sono stampati in grassetto e preceduti da un asterisco.

II

(Atti non legislativi)

REGOLAMENTI

REGOLAMENTO DI ESECUZIONE (UE) 2015/434 DELLA COMMISSIONE

del 16 marzo 2015

recante fissazione dei valori forfettari all'importazione ai fini della determinazione del prezzo di entrata di taluni ortofrutticoli

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il Regolamento (UE) n. 1308/2013 del Parlamento europeo e del Consiglio, del 17 dicembre 2013, recante organizzazione comune dei mercati dei prodotti agricoli e che abroga i regolamenti (CEE) n. 922/72, (CEE) n. 234/79, (CE) n. 1037/2001 e (CE) n. 1234/2007 del Consiglio ([1]),

visto il regolamento di esecuzione (UE) n. 543/2011 della Commissione, del 7 giugno 2011, recante modalità di applicazione del regolamento (CE) n. 1234/2007 del Consiglio nei settori degli ortofrutticoli freschi e degli ortofrutticoli trasformati ([2]), in particolare l'articolo 136, paragrafo 1,

considerando quanto segue:

(1) Il regolamento di esecuzione (UE) n. 543/2011 prevede, in applicazione dei risultati dei negoziati commerciali multilaterali dell'Uruguay round, i criteri per la fissazione da parte della Commissione dei valori forfettari all'importazione dai paesi terzi, per i prodotti e i periodi indicati nell'allegato XVI, parte A, del medesimo regolamento.

(2) Il valore forfettario all'importazione è calcolato ciascun giorno feriale, in conformità dell'articolo 136, paragrafo 1, del regolamento di esecuzione (UE) n. 543/2011, tenendo conto di dati giornalieri variabili. Pertanto il presente regolamento entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

I valori forfettari all'importazione di cui all'articolo 136 del regolamento di esecuzione (UE) n. 543/2011 sono quelli fissati nell'allegato del presente regolamento.

([1]) GU L 347 del 20.12.2013, pag. 671.
([2]) GU L 157 del 15.6.2011, pag. 1.

Articolo 2

Il presente regolamento entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 16 marzo 2015

Per la Commissione,
a nome del presidente
Jerzy PLEWA
Direttore generale dell'Agricoltura e dello sviluppo rurale

ALLEGATO

Valori forfettari all'importazione ai fini della determinazione del prezzo di entrata di taluni ortofrutticoli

(EUR/100 kg)

Codice NC	Codice dei paesi terzi ([1])	Valore forfettario all'importazione
0702 00 00	EG	65,8
	MA	84,9
	TR	86,4
	ZZ	79,0
0707 00 05	JO	229,9
	MA	183,9
	TR	185,1
	ZZ	199,6
0709 93 10	MA	119,5
	TR	192,4
	ZZ	156,0
0805 10 20	EG	45,8
	IL	72,7
	MA	56,7
	TN	57,3
	TR	63,6
	ZZ	59,2
0805 50 10	TR	61,4
	ZZ	61,4
0808 10 80	BR	70,9
	CA	81,0
	CL	100,9
	CN	91,1
	MK	25,2
	US	166,1
	ZZ	89,2
0808 30 90	AR	112,0
	CL	133,2
	US	124,8
	ZA	103,5
	ZZ	118,4

([1]) Nomenclatura dei paesi stabilita dal Regolamento (UE) n. 1106/2012 della Commissione, del 27 novembre 2012, che attua il regolamento (CE) n. 471/2009 del Parlamento europeo e del Consiglio, relativo alle statistiche comunitarie del commercio estero con i paesi terzi, per quanto riguarda l'aggiornamento della nomenclatura dei paesi e territori (GU L 328 del 28.11.2012, pag. 7). Il codice «ZZ» corrisponde a «altre origini».

DECISIONI

DECISIONE (UE) 2015/435 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 dicembre 2014

relativa alla mobilitazione del margine per imprevisti

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto l'accordo interistituzionale, del 2 dicembre 2013, tra il Parlamento europeo, il Consiglio e la Commissione sulla disciplina di bilancio, sulla cooperazione in materia di bilancio e sulla sana gestione finanziaria ([1]), in particolare il punto 14,

vista la proposta della Commissione europea,

considerando che:

(1) L'articolo 13 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio ([2]) ha fissato un margine per imprevisti che può arrivare fino allo 0,03 % del reddito nazionale lordo dell'Unione.

(2) Conformemente all'articolo 6 di tale regolamento, la Commissione ha calcolato l'importo assoluto del margine per imprevisti per il 2014 ([3]).

(3) Dopo avere esaminato tutte le altre possibilità finanziarie per reagire alle circostanze impreviste verificatesi dopo che il massimale dei pagamenti del quadro finanziario pluriennale per il 2014 è stato fissato per la prima volta nel febbraio 2013, risulta necessario mobilitare il margine per imprevisti per integrare gli stanziamenti di pagamento a titolo del bilancio generale dell'Unione europea per l'esercizio 2014, oltre il massimale di pagamento.

(4) Occorre includere nella mobilitazione del margine per imprevisti un importo di 350 milioni di EUR in stanziamenti di pagamento, in attesa di un accordo in merito ai pagamenti per gli altri strumenti speciali.

(5) Considerata la situazione estremamente particolare verificatasi quest'anno, si considerano soddisfatte le condizioni per ricorrere allo strumento di ultima istanza previsto all'articolo 13, paragrafo 1, del regolamento (UE, Euratom) n. 1311/2013.

(6) Per garantire il rispetto dell'articolo 13, paragrafo 3, del regolamento (UE, Euratom) n. 1311/2013, la Commissione dovrebbe presentare una proposta sulla detrazione dei pertinenti importi nei massimali di pagamento del QFP per uno o più esercizi futuri, tenendo debitamente conto degli accordi di pagamento relativi ad altri strumenti speciali, e fatte salve le prerogative istituzionali della Commissione,

([1]) GU C 373 del 20.12.2013, pag. 1.
([2]) Regolamento (UE, Euratom) n. 1311/2013 del Consiglio, del 2 dicembre 2013, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020 (GU L 347 del 20.12.2013, pag. 884).
([3]) Comunicazione della Commissione al Consiglio e al Parlamento europeo del 20 dicembre 2013: Adeguamento tecnico del quadro finanziario per il 2014 all'evoluzione dell'RNL [COM(2013) 928].

HANNO ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Nel quadro del bilancio generale dell'Unione europea per l'esercizio finanziario 2014, il margine per imprevisti è utilizzato per fornire la somma di 3 168 233 715 EUR in stanziamenti di pagamento al di sopra del massimale di pagamento del quadro finanziario pluriennale.

Articolo 2

La somma di 2 818 233 715 EUR è detratta in tre rate dai margini al di sotto dei massimali di pagamento per i seguenti anni:

a) 2018: 939 411 200 EUR

b) 2019: 939 411 200 EUR

c) 2020: 939 411 315 EUR

Si invita la Commissione a presentare in tempo utile una proposta concernente il rimanente importo di 350 milioni di EUR.

Articolo 3

La presente decisione è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Strasburgo, il 17 dicembre 2014

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	B. DELLA VEDOVA

DECISIONE (UE) 2015/436 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 dicembre 2014

concernente la mobilitazione del Fondo di solidarietà dell'Unione europea

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (CE) n. 2012/2002 del Consiglio, dell'11 novembre 2002, che istituisce il Fondo di solidarietà dell'Unione europea ([1]), in particolare l'articolo 4, paragrafo 3,

visto l'accordo interistituzionale, del 2 dicembre 2013, tra il Parlamento europeo, il Consiglio e la Commissione sulla disciplina di bilancio, sulla cooperazione in materia di bilancio e sulla sana gestione finanziaria ([2]), in particolare il punto 11,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) L'Unione europea ha istituito il Fondo di solidarietà dell'Unione europea (di seguito il «Fondo») per testimoniare la propria solidarietà alle popolazioni delle regioni colpite da catastrofi.

(2) L'articolo 10 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio ([3]), consente di mobilitare il Fondo nei limiti di un massimale annuo pari a 500 milioni di EUR (ai prezzi del 2011).

(3) Il regolamento (CE) n. 2012/2002 contiene le disposizioni che disciplinano la mobilitazione del Fondo.

(4) L'Italia ha presentato richiesta di mobilitazione del Fondo in relazione a inondazioni.

(5) La Grecia ha presentato richiesta di mobilitazione del Fondo in relazione ad un terremoto.

(6) La Slovenia ha presentato richiesta di mobilitazione del Fondo in relazione a tempeste di ghiaccio.

(7) La Croazia ha presentato richiesta di mobilitazione del Fondo in relazione a tempeste di ghiaccio seguite da inondazioni,

HANNO ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Nel quadro del bilancio generale dell'Unione europea fissato per l'esercizio 2014, una somma pari a 46 998 528 EUR di stanziamenti d'impegno è mobilitata a titolo del Fondo di solidarietà dell'Unione europea.

Nel quadro del bilancio generale dell'Unione europea fissato per l'esercizio 2015, una somma pari a 46 998 528 EUR di stanziamenti di pagamento è mobilitata a titolo del Fondo di solidarietà dell'Unione europea.

Articolo 2

La presente decisione è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Strasburgo, il 17 dicembre 2014

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	B. DELLA VEDOVA

([1]) GU L 311 del 14.11.2002, pag. 3.
([2]) GU C 373 del 20.12.2013, pag. 1.
([3]) Regolamento (UE, Euratom) n. 1311/2013 del Consiglio, del 2 dicembre 2013, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020 (GU L 347 del 20.12.2013, pag. 884).

DECISIONE (UE) 2015/437 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 17 dicembre 2014

concernente la mobilitazione del Fondo di solidarietà dell'Unione europea

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (CE) n. 2012/2002 del Consiglio, dell'11 novembre 2002, che istituisce il Fondo di solidarietà dell'Unione europea ([1]), in particolare l'articolo 4, paragrafo 3,

visto l'accordo interistituzionale, del 2 dicembre 2013, tra il Parlamento europeo, il Consiglio e la Commissione sulla disciplina di bilancio, sulla cooperazione in materia di bilancio e sulla sana gestione finanziaria ([2]), in particolare il punto 11,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) L'Unione europea ha istituito il Fondo di solidarietà dell'Unione europea (il «Fondo») per testimoniare solidarietà alla popolazione di regioni colpite da catastrofi.

(2) L'articolo 10 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio ([3]) consente di mobilitare il Fondo nei limiti di un massimale annuo pari a 500 milioni di EUR (ai prezzi del 2011).

(3) Il regolamento (CE) n. 2012/2002 contiene le disposizioni che disciplinano la mobilitazione del Fondo.

(4) La Serbia ha presentato richiesta di mobilitazione del Fondo in relazione a inondazioni.

(5) La Croazia ha presentato richiesta di mobilitazione del Fondo in relazione a inondazioni.

(6) La Bulgaria ha presentato richiesta di mobilitazione del Fondo in relazione a inondazioni,

HANNO ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Nel quadro del bilancio generale dell'Unione europea fissato per l'esercizio 2014, una somma pari a 79 726 440 EUR di stanziamenti di impegno è mobilitata a titolo del Fondo di solidarietà dell'Unione europea.

Nel quadro del bilancio generale dell'Unione europea fissato per l'esercizio 2015, una somma pari a 79 726 440 EUR di stanziamenti di pagamento è mobilitata a titolo del Fondo di solidarietà dell'Unione europea.

Articolo 2

La presente decisione è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Strasburgo, il 17 dicembre 2014

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	B. DELLA VEDOVA

([1]) GU L 311 del 14.11.2002, pag. 3.
([2]) GU C 373 del 20.12.2013, pag. 1.
([3]) Regolamento (UE, Euratom) n. 1311/2013 del Consiglio, del 2 dicembre 2013, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020 (GU L 347 del 20.12.2013, pag. 884).

DECISIONE (UE) 2015/438 DEL CONSIGLIO

del 2 marzo 2015

che stabilisce la posizione che dev'essere adottata a nome dell'Unione europea in sede di comitato misto istituito ai sensi dell'accordo fra l'Unione europea e l'Ucraina di facilitazione del rilascio dei visti, sull'adozione degli orientamenti comuni per l'attuazione dell'accordo

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 77, paragrafo 2, lettera a), in combinato disposto con l'articolo 218, paragrafo 9,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) L'articolo 12 dell'accordo fra l'Unione europea e l'Ucraina di facilitazione del rilascio dei visti ([1]) («accordo») istituisce un comitato misto e prevede che esso debba, in particolare, controllare l'applicazione dell'accordo.

(2) L'accordo fra l'Unione europea e l'Ucraina che modifica l'accordo fra la Comunità europea e l'Ucraina di facilitazione del rilascio dei visti ([2]) («accordo di modifica») è entrato in vigore il 1º luglio 2013.

(3) Il regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio ([3]) ha istituito le procedure e le condizioni per il rilascio dei visti di transito o per soggiorni previsti di non più di 90 giorni su un periodo di 180 giorni nel territorio degli Stati membri.

(4) Nell'ambito dela sua responsabilità, il comitato misto ha rilevato l'esigenza di orientamenti comuni per garantire che i consolati degli Stati membri applichino l'accordo in modo del tutto armonizzato e per chiarire la relazione fra le disposizioni dell'accordo e le disposizioni delle parti contraenti che continuano ad applicarsi alle questioni in materia di visti non contemplate dall'accordo.

(5) Il comitato misto ha adottato tali orientamenti il 25 novembre 2009 con la decisione n. 1/2009. Tali orientamenti dovrebbero essere adattati alle nuove disposizioni dell'accordo di modifica e ai cambiamenti nel diritto interno dell'Unione sulla politica dei visti. Per chiarezza è opportuno sostituire tali orientamenti.

(6) È opportuno stabilire la posizione che dev'essere adottata in sede di comitato misto sull'adozione degli orientamenti comuni per l'attuazione dell'accordo,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La posizione che deve essere adottata a nome dell'Unione in sede di comitato misto istituito dall'articolo 12 dell'accordo fra l'Unione europea e l'Ucraina di facilitazione del rilascio dei visti, sull'adozione degli orientamenti comuni per l'attuazione dell'accordo, si basa sul progetto di decisione del comitato misto accluso alla presente decisione.

([1]) GU L 332 del 18.12.2007, pag. 68.
([2]) GU L 168 del 20.6.2013, pag. 11.
([3]) Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

Articolo 2

La presente decisione entra in vigore alla data di adozione.

Fatto a Bruxelles, il 2 marzo 2015

Per il Consiglio
Il presidente
D. REIZNIECE-OZOLA

PROGETTO di

DECISIONE N. …/2014 DEL COMITATO MISTO ISTITUITO DALL'ACCORDO FRA L'UNIONE EUROPEA E L'UCRAINA DI FACILITAZIONE DEL RILASCIO DEI VISTI

del …

sull'adozione degli orientamenti comuni per l'attuazione dell'accordo

IL COMITATO MISTO,

visto l'accordo fra l'Unione europea e l'Ucraina di facilitazione del rilascio dei visti («accordo»), in particolare l'articolo 12,

considerando che l'accordo è entrato in vigore il 1º gennaio 2008,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Gli orientamenti comuni per l'attuazione dell'accordo fra l'Unione europea e l'Ucraina di facilitazione del rilascio dei visti sono fissati nell'allegato della presente decisione.

Articolo 2

La decisione n. 1/2009 del comitato misto è abrogata.

Articolo 3

La presente decisione entra in vigore il giorno dell'adozione.

Fatto a …,

Per l'Unione europea *Per l'Ucraina*

ALLEGATO

ORIENTAMENTI COMUNI PER L'ATTUAZIONE DELL'ACCORDO FRA L'UNIONE EUROPEA E L'UCRAINA DI FACILITAZIONE DEL RILASCIO DEI VISTI

Scopo dell'accordo di facilitazione del rilascio dei visti fra l'Unione europea e l'Ucraina, entrato in vigore il 1º gennaio 2008, quale modificato dall'accordo fra l'Unione europea e l'Ucraina del 23 luglio 2012, entrato in vigore il 1º luglio 2013 («accordo»), è agevolare, su una base di reciprocità, le procedure di rilascio di visti ai cittadini ucraini per soggiorni previsti di massimo 90 giorni per periodi di 180 giorni.

L'accordo istituisce, su una base di reciprocità, diritti e obblighi giuridicamente vincolanti allo scopo di semplificare le procedure di rilascio del visto ai cittadini ucraini.

I presenti orientamenti, adottati dal comitato misto istituito dall'articolo 12 dell'accordo («comitato misto»), sono volti a garantire un'attuazione corretta e armonizzata delle disposizioni dell'accordo da parte delle rappresentanze diplomatiche e consolari degli Stati membri. Tali orientamenti non sono parte dell'accordo e non sono pertanto giuridicamente vincolanti. Tuttavia, è fortemente raccomandato che il personale diplomatico e consolare vi si attenga in modo coerente quando applica le disposizioni dell'accordo.

I presenti orientamenti sono intesi ad aggiornare alla luce dell'esperienza acquisita nell'attuazione dell'accordo sotto la responsabilità del comitato misto. Gli orientamenti adottati dal comitato misto il 25 novembre 2009 sono stati adattati in linea con l'accordo fra l'Unione europea e l'Ucraina che modifica l'accordo tra la Comunità europea e l'Ucraina di facilitazione del rilascio dei visti («accordo di modifica»), e con nuovi atti normativi dell'Unione come il regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio ([1]) («codice dei visti»).

I. ASPETTI GENERALI

1.1. **Scopo e ambito d'applicazione**

L'articolo 1 dell'accordo recita come segue: «Scopo del presente accordo è agevolare il rilascio di visti ai cittadini ucraini per soggiorni previsti di massimo 90 giorni per periodi di 180 giorni.».

L'accordo si applica a tutti i cittadini ucraini che presentano domanda per visti per soggiorni di breve durata, qualunque sia il paese in cui risiedono.

Ai sensi dell'articolo 1, paragrafo 2, dell'accordo, l'«Ucraina può reintrodurre l'obbligo di visto solo per i cittadini, o per determinate categorie di cittadini, di tutti gli Stati membri, e non per i cittadini o per determinate categorie di cittadini di singoli Stati membri. Se l'Ucraina reintrodurrà l'obbligo di visto per i cittadini UE, o determinate categorie di cittadini UE, a questi si applicheranno automaticamente le medesime facilitazioni concesse dal presente accordo ai cittadini ucraini, per reciprocità.».

In base alle decisioni adottate dal governo ucraino, dal 1º maggio 2005 o, rispettivamente, dal 1º gennaio 2008, i cittadini UE che si recano in Ucraina per un periodo massimo di 90 giorni o che transitano per il territorio ucraino sono esenti dall'obbligo di visto. Questa disposizione non incide sul diritto del governo ucraino di modificare tali decisioni.

1.2. **Ambito d'applicazione dell'accordo.**

L'articolo 2 dell'accordo prevede quanto segue:

> «1. Le facilitazioni del visto previste nel presente accordo si applicano ai cittadini ucraini solo se gli stessi non sono esenti dall'obbligo di visto in virtù delle disposizioni legislative e regolamentari dell'Unione europea o degli Stati membri, del presente accordo o di altri accordi internazionali.
>
> 2. Le questioni non contemplate dalle disposizioni del presente accordo, quali il rifiuto del visto, il riconoscimento dei documenti di viaggio, la prova della sufficienza dei mezzi di sussistenza, il rifiuto dell'ingresso e i provvedimenti di allontanamento, sono disciplinate dal diritto nazionale dell'Ucraina o degli Stati membri o dal diritto dell'Unione europea.».

([1]) Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

Fatto salvo il suo articolo 10 (che prevede l'esenzione dall'obbligo di visto per i titolari di passaporti diplomatici e passaporti di servizio biometrici dell'Ucraina), l'accordo lascia invariate le norme esistenti in materia di obblighi di visto e di esenzioni dal visto. Ad esempio, l'articolo 4 del regolamento (CE) n. 539/2001 del Consiglio ([1]) consente agli Stati membri di esentare dall'obbligo del visto alcune categorie fra cui i membri degli equipaggi civili di aerei e navi.

Tutte le questioni non contemplate dall'accordo, quali il rifiuto del visto, il riconoscimento dei documenti di viaggio, la prova della sufficienza dei mezzi di sussistenza, il rifiuto dell'ingresso e i provvedimenti di allontanamento, continuano a essere disciplinate dalle norme Schengen e, se del caso, dal diritto nazionale. Ciò si applica anche alle norme Schengen che determinano lo Stato membro Schengen responsabile del trattamento di una domanda di visto. Pertanto, un cittadino ucraino dovrebbe continuare a chiedere il visto presso il consolato dello Stato membro in cui si trova la destinazione principale del suo viaggio; se non vi è una destinazione principale, dovrebbe presentare la domanda presso il consolato dello Stato membro del primo ingresso nello spazio Schengen.

Anche quando ricorrono le condizioni previste dall'accordo, ad esempio, il richiedente dimostra con prove documentali circa la finalità del viaggio secondo le categorie di cui al suo articolo 4, il rilascio del visto può sempre essere rifiutato se non sono soddisfatte le condizioni di cui all'articolo 5 del regolamento (CE) n. 562/2006 del Parlamento europeo e del Consiglio ([2]) («codice frontiere Schengen»),vale a dire se la persona non è in possesso di un documento di viaggio valido, se è segnalata nel SIS, se è considerata una minaccia per l'ordine pubblico, la sicurezza interna ecc.

Continuano ad applicarsi le altre possibilità di flessibilità nel rilascio dei visti consentite dal codice dei visti. Ad esempio, se ricorrono le condizioni previste dal codice dei visti (cfr. l'articolo 24, paragrafo 2, del codice dei visti), visti per ingressi multipli con un lungo periodo di validità fino a 5 anni possono essere rilasciati anche a categorie di persone diverse da quelle menzionate all'articolo 5 dell'accordo. Parimenti, continueranno ad applicarsi le disposizioni contenute nel codice dei visti riguardanti l'esenzione dal pagamento dei diritti di visto o la loro riduzione (cfr. II.2.1.1).

1.3. **Tipi di visto rientranti nell'ambito d'applicazione dell'accordo**

L'articolo 3, lettera d), dell'accordo definisce il «visto» come un'«autorizzazione rilasciata o una decisione presa da uno Stato membro per consentire:

— l'ingresso per un soggiorno previsto di massimo 90 giorni in totale nel territorio di quello Stato membro o di più Stati membri;

— l'ingresso per il transito nel territorio di quello Stato membro o di più Stati membri;».

L'accordo contempla il seguente tipo di visto:

— visto «C» (visto per soggiorni di breve durata).

Le facilitazioni previste dall'accordo si applicano sia ai visti uniformi validi per l'intero territorio degli Stati membri sia ai visti con validità territoriale limitata (VTL).

1.4. **Calcolo della durata del soggiorno autorizzato da un visto e, in particolare, questione del calcolo del periodo di sei mesi**

La recente modifica del codice frontiere Schengen ha ridefinito il concetto di soggiorno di breve durata. La definizione attuale è la seguente: «90 giorni su un periodo di 180 giorni, il che comporta di prendere in considerazione il periodo di 180 giorni che precede ogni giorno di soggiorno».

Il giorno dell'ingresso sarà calcolato come il primo giorno di soggiorno nel territorio degli Stati membri e il giorno dell'uscita sarà calcolato come l'ultimo giorno di soggiorno nel territorio degli Stati membri. Questo concetto implica l'applicazione di un periodo di riferimento «mobile» di 180 giorni: per ogni giorno del soggiorno si guarda indietro all'ultimo periodo di 180 giorni, per verificare se il requisito dei 90/180 giorni continua a essere rispettato. Ciò significa che un'assenza per un periodo ininterrotto di 90 giorni consente un nuovo soggiorno fino a 90 giorni.

La definizione è entrata in vigore il 18 ottobre 2013. Il calcolatore si trova on line al seguente indirizzo: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm.

([1]) Regolamento (CE) n. 539/2001 del Consiglio, del 15 marzo 2001, che adotta l'elenco dei paesi terzi i cui cittadini devono essere in possesso del visto all'atto dell'attraversamento delle frontiere esterne e l'elenco dei paesi terzi i cui cittadini sono esenti da tale obbligo (GU L 81 del 21.3.2001, pag. 1).

([2]) Regolamento (CE) n. 562/2006 del Parlamento europeo e del Consiglio, del 15 marzo 2006, che istituisce un codice comunitario relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen) (GU L 105 del 13.4.2006, pag. 1).

Esempio di calcolo del soggiorno in base alla nuova definizione:

Una persona in possesso di un visto per più ingressi con validità di 1 anno (18.4.2014-18.4.2015) entra per la prima volta il 19.4.2014 e soggiorna 3 giorni. Entra nuovamente il 18.6.2014 e soggiorna 86 giorni. Qual è la situazione in determinate date? Quando sarà consentito nuovamente l'ingresso all'interessato?

In data 11.9.2014: negli ultimi 180 giorni (16.3.2014-11.9.2014) la persona ha soggiornato per 3 giorni (19-21.4.2014) più 86 giorni (18.6.2014-11.9.2014) = 89 giorni = nessun prolungamento indebito del soggiorno. La persona può ancora soggiornare 1 giorno.

In data 16.10.2014: la persona potrebbe rientrare per un periodo di 3 giorni supplementari (in data 16.10.2014 il soggiorno effettuato il giorno 19.4.2014 diventa irrilevante ai fini del calcolo, trovandosi al di fuori del periodo di 180 giorni; in data 17.10.2014 il soggiorno effettuato il giorno 20.4.2014 diventa irrilevante ai fini del calcolo, trovandosi al di fuori del periodo di 180 giorni; e così di seguito).

In data 15.12.2014: la persona potrebbe rientrare per un periodo di 86 giorni (in data 15.12.2014, il soggiorno effettuato il giorno 18.6.2014 diventa irrilevante ai fini del calcolo, trovandosi al di fuori del periodo di 180 giorni; in data 16.12.2014 il soggiorno effettuato il giorno 19.6.2014 diventa irrilevante, e così di seguito).

1.5. **Situazione relativa agli Stati membri che non applicano ancora integralmente l'acquis di Schengen, agli Stati membri che non partecipano alla politica comune dell'UE in materia di visti e ai paesi associati.**

Gli Stati membri che hanno aderito all'Unione nel 2004 (Repubblica ceca, Estonia, Cipro, Lettonia, Lituania, Ungheria, Malta, Polonia, Slovenia e Slovacchia), nel 2007 (Bulgaria e Romania) e nel 2013 (Croazia) sono vincolati dall'accordo dalla data della sua entrata in vigore.

Solo la Bulgaria, la Croazia, Cipro e la Romania non applicano ancora integralmente l'acquis di Schengen e continueranno a rilasciare visti nazionali con una validità limitata al loro territorio nazionale. Quando questi Stati membri applicheranno integralmente l'acquis di Schengen, continueranno ad applicare l'accordo.

Il diritto nazionale continua ad applicarsi a tutte le questioni non contemplate dall'accordo fino alla data della piena applicazione dell'acquis di Schengen da parte di tali Stati membri. Da tale data, le questioni non regolate dall'accordo saranno disciplinate dalle norme Schengen/dal diritto nazionale.

La Bulgaria, la Croazia, Cipro e la Romania sono autorizzati a riconoscere i permessi di soggiorno, i visti di tipo D e i visti per soggiorni di breve durata rilasciati dagli Stati Schengen e dai paesi associati per soggiorni di breve durata sul loro territorio.

Conformemente all'articolo 21 della convenzione di applicazione dell'accordo di Schengen, del 14 giugno 1985, sulla graduale eliminazione dei controlli alle frontiere comuni, tutti gli Stati Schengen devono riconoscere i visti per soggiorni di lunga durata e i permessi di soggiorno rilasciati dagli altri Stati Schengen come validi per soggiorni di breve durata sui rispettivi territori. Gli Stati membri Schengen accettano i permessi di soggiorno, i visti di tipo D e i visti per soggiorni di breve durata dei paesi associati ai fini dell'ingresso e di soggiorni di breve durata, e viceversa.

L'accordo non si applicaalla Danimarca, all'Irlanda e al Regno Unito, ma include dichiarazioni comuni sull'auspicabilità della conclusione di accordi bilaterali sulla facilitazione del rilascio dei visti fra tali Stati membri e l'Ucraina.

Un accordo bilaterale sulla facilitazione del visto fra la Danimarca e l'Ucraina è entrato in vigore il 1º marzo 2009. Non si è svolto alcun negoziato sulla facilitazione del visto fra l'Ucraina e, rispettivamente, l'Irlanda e il Regno Unito.

L'accordo non si applica all'Islanda, al Liechtenstein, alla Norvegia e alla Svizzera, pur essendo questi paesi associati a Schengen, ma comprende dichiarazioni comuni sull'auspicabilità di tali paesi Schengen di concludere accordi bilaterali sulla facilitazione del rilascio dei visti con l'Ucraina.

La Norvegia ha firmato un accordo bilaterale di facilitazione del rilascio dei visti il 13 febbraio 2008. Tale accordo è entrato in vigore il 1º settembre 2011.

La Svizzera ha finalizzato i negoziati per un accordo bilaterale di facilitazione del rilascio dei visti nel novembre 2011. L'Islanda ha indicato che i negoziati con l'Ucraina sono cominciati.

1.6. **Accordi bilaterali**

L'articolo 13, paragrafo 1, dell'accordo prevede quanto segue:

> «1. Sin dall'entrata in vigore del presente accordo, le disposizioni ivi contenute prevalgono su quelle di qualsiasi accordo o intesa bilaterale o multilaterale vigente tra i singoli Stati membri e l'Ucraina, nella misura in cui queste ultime disposizioni abbiano il medesimo oggetto dell'accordo.».

Dalla data di entrata in vigore dell'accordo, le disposizioni degli accordi bilaterali in vigore fra gli Stati membri e l'Ucraina sulle questioni contemplate dall'accordo cessano di applicarsi. Conformemente al diritto dell'Unione, gli Stati membri devono adottare le disposizioni necessarie per eliminare le incompatibilità fra i loro accordi bilaterali e l'accordo.

Tuttavia, l'articolo 13, paragrafo 2, dell'accordo prevede quanto segue:

> «2. Le disposizioni degli accordi o delle intese bilaterali in vigore fra i singoli Stati membri e l'Ucraina conclusi prima dell'entrata in vigore del presente accordo e che prevedono l'esenzione dall'obbligo del visto per i titolari di passaporti di servizio non biometrici continuano ad applicarsi fermo restando il diritto degli Stati membri interessati o dell'Ucraina di denunciare o sospendere tali accordi o intese bilaterali.».

I seguenti Stati membri hanno stipulato un accordo bilaterale con l'Ucraina che prevede l'esenzione dall'obbligo del visto per i titolari di passaporti di servizio: Bulgaria, Croazia, Cipro, Lettonia, Lituania, Ungheria, Polonia, Romania e Slovacchia.

Conformemente all'articolo 13, paragrafo 1, dell'accordo, nella misura in cui tali accordi bilaterali riguardano i passaporti di servizio biometrici, l'articolo 10, paragrafo 2, dell'accordo prevale su tali accordi bilaterali. Conformemente all'articolo 13, paragrafo 2, dell'accordo, tali accordi bilaterali, conclusi prima dell'entrata in vigore dell'accordo di modifica, continueranno ad applicarsi nella misura in cui riguardano i titolari di passaporti di servizio non biometrici, fermo restando il diritto degli Stati membri interessati o dell'Ucraina di denunciare o sospendere tali accordi o intese bilaterali. L'esenzione dal visto per i titolari di passaporti di servizio non biometrici accordata da uno Stato membro si applica solo per il viaggio sul territorio di tale Stato membro, e non per recarsi negli altri Stati membri Schengen.

Se uno Stato membro ha concluso un accordo o un'intesa bilaterale con l'Ucraina su questioni non contemplate dall'accordo, tale esenzione continua ad applicarsi dopo l'entrata in vigore dell'accordo.

1.7. **Dichiarazione della Comunità europea sull'accesso dei richiedenti il visto alle informazioni riguardanti le procedure di rilascio dei visti per soggiorni di breve durata e relativa armonizzazione, e sulla documentazione da allegare alla domanda di visto di soggiorno di breve durata**

Conformemente a tale dichiarazione della Comunità europea acclusta all'accordo, per garantire che i richiedenti il visto abbiano a disposizione dati coerenti e uniformi, sono state redatte informazioni comuni di base sull'accesso alle rappresentanze diplomatiche e consolari degli Stati membri, sulle procedure e sulle condizioni relative al rilascio dei visti e sulla validità dei visti rilasciati. Tali informazioni sono disponibili sul sito web della delegazione UE in Ucraina (http://eeas.europa.eu/delegations/ukraine/index_en.htm).

Le rappresentanze diplomatiche e consolari degli Stati membri sono tenute a divulgare ampiamente queste informazioni (nelle bacheche, negli opuscoli, sui siti web. ecc.) e a divulgare anche informazioni precise sulle condizioni del rilascio dei visti, sulle rappresentanze degli Stati membri in Ucraina e sull'elenco UE armonizzato della documentazione giustificativa richiesta.

II. ORIENTAMENTI SU DISPOSIZIONI SPECIFICHE

2.1. **Norme applicabili a tutti i richiedenti il visto**

Importante; si ricorda che le facilitazioni sotto indicate, riguardanti i diritti e i termini per il trattamento delle domande di visto, la partenza in caso di smarrimento o furto dei documenti, e i casi eccezionali di proroga del visto, si applicano a tutti i richiedenti e a tutti i titolari di visto ucraini.

2.1.1. *Diritti per il trattamento delle domande di visto*

L'articolo 6, paragrafo 1, dell'accordo prevede quanto segue:

> «I diritti per il trattamento delle domande di visto dei cittadini ucraini ammontano a 35 EUR. Tale importo può essere rivisto secondo la procedura di cui all'articolo 14, paragrafo 4.».

Conformemente all'articolo 6, paragrafo 1, i diritti per il trattamento di una domanda di visto sono pari a 35 EUR. Tali diritti si applicano a tutti i richiedenti il visto ucraini (compresi i turisti), riguardano i visti per soggiorni di breve durata, indipendentemente dal numero di ingressi, e si applicano anche alle domande di visto presentate alle frontiere esterne.

L'articolo 6, paragrafo 2, dell'accordo prevede quanto segue:

> «Se l'Ucraina reintrodurrà l'obbligo del visto per i cittadini UE, i diritti che potrà esigere non dovranno essere superiori a 35 EUR ovvero all'importo convenuto se i diritti sono rivisti secondo la procedura di cui all'articolo 14, paragrafo 4.».

L'articolo 6, paragrafo 3, dell'accordo prevede quanto segue:

> «Gli Stati membri applicano diritti pari a 70 EUR per il trattamento dei visti qualora il richiedente, tenuto conto della distanza fra il suo luogo di residenza e quello di presentazione della domanda, chieda l'adozione di una decisione entro tre giorni dalla presentazione della domanda, e il consolato accetti.».

I diritti di 70 EUR saranno applicati per il trattamento delle domande di visto nei casi in cui la domanda e i documenti giustificativi siano stati presentati da un richiedente il cui luogo di residenza si trova in un *oblast* in cui lo Stato membro di destinazione non ha una rappresentanza consolare (vale a dire se in tale *oblast* non c'è nessun consolato, nessun centro per i visti, né alcun consolato di Stati membri che abbiano concluso accordi di rappresentanza con lo Stato membro in cui il richiedente intende recarsi), e se la rappresentanza diplomatica o consolare ha convenuto di adottare una decisione sulla domanda di visto entro tre giorni. Le prove riguardanti il luogo di residenza del richiedente il visto sono fornite col modulo di domanda di visto.

In linea di principio, l'articolo 6, paragrafo 3, dell'accordo serve a facilitare la presentazione della domanda di visto ai richiedenti che vivono molto lontano dal consolato e devono effettuare un viaggio lungo per presentare la domanda: lo scopo è che il visto sia rilasciato in tempi brevi in modo che possano riceverlo senza dover compiere lo stesso impegnativo spostamento una seconda volta.

Per le ragioni sopra indicate, nei casi in cui i tempi di trattamento «standard» di una domanda di visto da parte di una data rappresentanza diplomatica o consolare siano di tre giorni o meno, saranno applicati i diritti standard di 35 EUR.

Per le rappresentanze diplomatiche e consolari che hanno un sistema di appuntamenti, il periodo di tempo per ottenere l'appuntamento non è calcolato come parte del tempo di trattamento (cfr. anche II.2.1.2).

L'articolo 6, paragrafo 4, dell'accordo prevede quanto segue:

> «4. Fermo restando il paragrafo 5, sono esenti dai diritti per il trattamento delle domande di visto le seguenti categorie di persone:
>
> a) i parenti stretti — coniugi, figli (anche adottivi), genitori (anche tutori), nonni e nipoti — di cittadini ucraini regolarmente soggiornanti nel territorio degli Stati membri o di cittadini dell'Unione europea che risiedono nel territorio dello Stato membro di cui hanno la cittadinanza;»

(N.B. Tale punto disciplina la situazione dei parenti stretti ucraini che si recano in Stati membri in visita a cittadini ucraini regolarmente soggiornanti negli Stati membri o a cittadini dell'Unione europea residenti nel territorio dello Stato membro di cui hanno la cittadinanza. Ai richiedenti il visto ucraini familiari di un cittadino dell'Unione, ai sensi dell'articolo 5, paragrafo 2, della direttiva 2004/38/CE del Parlamento europeo e del Consiglio ([1]), saranno rilasciati visti gratuiti, il più presto possibile e in base a una procedura accelerata.)

> «b) i membri di delegazioni ufficiali che, su invito ufficiale rivolto all'Ucraina, partecipano a riunioni, consultazioni, negoziati o programmi di scambio, o a eventi organizzati nel territorio di uno Stato membro da organizzazioni intergovernative;
>
> c) i membri di governi e parlamenti nazionali e regionali e i membri di corti costituzionali e di tribunali di ultimo grado che non siano esenti dall'obbligo di visto in virtù del presente accordo;
>
> d) gli studenti di scuole inferiori e superiori, di università o corsi post-universitari e i docenti accompagnatori in viaggio di studio o di formazione;
>
> e) i disabili ed eventuali accompagnatori» (N.B. — Per beneficiare dell'esenzione dai diritti occorre dimostrare che ogni richiedente il visto rientra in questa categoria.)
>
> «f) le persone che hanno documentato la necessità del viaggio per motivi umanitari, inclusa la necessità di ricevere trattamenti medici urgenti (nel qual caso l'esonero è esteso agli accompagnatori) o di partecipare al funerale di un parente stretto o di visitare un parente stretto gravemente malato;
>
> g) i partecipanti a eventi sportivi internazionali e gli accompagnatori» (N.B. — Sono contemplati solo gli accompagnatori che viaggiano a titolo professionale; i tifosi non saranno considerati accompagnatori.)

([1]) Direttiva 2004/38/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri, che modifica il regolamento (CEE) n. 1612/68 e abroga le direttive 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (GU L 158 del 30.4.2004, pag. 77).

«h) i partecipanti ad attività scientifiche, culturali e artistiche, inclusi i programmi di scambi universitari o di altro tipo;

i) i partecipanti a programmi di scambio ufficiali organizzati da città gemellate e da altre entità municipali;

j) i giornalisti e il personale tecnico che li accompagna a titolo professionale;» (N.B. — Sono contemplati dal presente punto i giornalisti di cui all'articolo 4, paragrafo 1, lettera e).);

«k) i pensionati» (N.B. — Per poter beneficiare dell'esenzione dal visto per questa categoria, i richiedenti devono dimostrare lo status di pensionati.)

«l) gli autotrasportatori che effettuano servizi di trasporto internazionale di merci e passeggeri nel territorio degli Stati membri con veicoli immatricolati in Ucraina;

m) il personale di carrozza, di locomotiva o addetto ai vagoni frigoriferi di treni internazionali che viaggiano nei territori degli Stati membri;

n) i minori di anni 18 e i figli a carico di età inferiore a 21 anni;» (N.B. — Per poter beneficiare dell'esenzione dal visto per questa categoria, i richiedenti devono presentare documenti che dimostrino l'età e — se inferiore a 21 anni — lo status di figli a carico);

«o) i rappresentanti di comunità religiose;

p) i liberi professionisti che partecipano a fiere, conferenze, convegni, seminari internazionali o altri eventi analoghi organizzati nel territorio degli Stati membri;

q) i giovani di età non superiore a venticinque anni che partecipano a seminari, conferenze e manifestazioni sportive, culturali o formative organizzate da associazioni senza scopo di lucro;

r) i rappresentanti di organizzazioni della società civile che effettuano viaggi finalizzati a seguire formazioni, seminari e conferenze, anche nel quadro di programmi di scambio;

s) i partecipanti a programmi ufficiali di cooperazione transfrontaliera dell'Unione europea, come ad esempio lo strumento europeo di vicinato e partenariato (ENPI).

Il primo comma si applica anche quando lo scopo del viaggio è il transito.».

L'articolo 6, paragrafo 4, secondo comma, dell'accordo si applica solo se lo scopo del viaggio nel paese terzo è equivalente a una delle finalità elencate all'articolo 6, paragrafo 4, lettere da a) a s), dell'accordo, ad esempio se il transito è necessario per partecipare a un seminario, per recarsi in visita presso familiari, per partecipare a programmi di scambio di organizzazioni della società civile ecc., nel paese terzo.

Le categorie di persone sopra menzionate sono del tutto esenti dal pagamento dei diritti. Inoltre, conformemente all'articolo 16, paragrafo 6, del codice dei visti, «[i]n singoli casi è possibile derogare alla riscossione o ridurre l'importo dei diritti per i visti, quando ciò serve a promuovere gli interessi culturali o sportivi, nonché gli interessi in materia di politica estera, di politica dello sviluppo e di altri settori essenziali d'interesse pubblico o per motivi umanitari.».

Tuttavia, questa regola non può essere applicata ai fini dell'esenzione dai diritti di trattamento di 70 EUR nei singoli in casi in cui la domanda di visto e i documenti giustificativi sono stati presentati da un richiedente il cui luogo di residenza è molto lontano dalla rappresentanza diplomatica o consolare dello Stato membro, pur appartenendo a una delle categorie esenti dai diritti per il visto di cui all'articolo 6, paragrafo 4, dell'accordo.

Va inoltre ricordato che le categorie di persone esenti dal pagamento dei diritti per il visto potrebbero comunque essere tenute a corrispondere un diritto per servizi nel caso in cui lo Stato membro cooperi con un fornitore esterno di servizi.

Ai sensi dell'articolo 6, paragrafo 5, dell'accordo:

«5. Se uno Stato membro coopera con un fornitore esterno di servizi ai fini del rilascio dei visti, tale fornitore esterno può applicare un diritto per servizi. Tale diritto è proporzionato ai costi sostenuti dal fornitore esterno per assolvere ai suoi compiti e non può essere superiore a 30 EUR. Gli Stati membri mantengono la possibilità, per tutti i richiedenti, di presentare la domanda di visto direttamente ai rispettivi consolati. Se i richiedenti sono tenuti a ottenere un appuntamento per la presentazione della domanda, tale appuntamento, di norma, ha luogo entro due settimane da quando viene chiesto.».

Mantenere la possibilità, per tutte le categorie di richiedenti il visto, di presentare domanda direttamente al consolato invece che tramite un fornitore esterno di servizi significa che dovrebbe esserci un'effettiva scelta fra queste due possibilità. Anche se l'accesso diretto non deve necessariamente essere organizzato a condizioni identiche o simili a quelle per l'accesso al fornitore di servizi, tali condizioni non devono rendere l'accesso diretto impossibile nella pratica. Anche se è accettabile avere tempi d'attesa diversi per ottenere un appuntamento in caso di accesso diretto, tali tempi d'attesa non devono essere così lunghi da rendere, in pratica, impossibile tale accesso diretto.

2.1.2. *Termini per il trattamento delle domande di visto.*

L'articolo 7 dell'accordo stabilisce quanto segue:

> «1. Le rappresentanze diplomatiche e consolari degli Stati membri decidono sulla domanda di rilascio del visto entro 10 giorni di calendario dalla data di ricevimento della domanda e della documentazione necessaria per il rilascio del visto.
>
> 2. In singoli casi, qualora si debba procedere a un ulteriore esame della domanda, il termine per decidere può essere prorogato fino a 30 giorni di calendario.
>
> 3. In casi urgenti il termine per decidere sulla domanda di visto può essere ridotto a due giorni lavorativi o a un periodo inferiore.».

Una decisione su una domanda di visto verrà presa, in linea di principio, entro 10 giorni di calendario dalla data di ricevimento della domanda di visto completa e dei documenti giustificativi.

Questo termine può essere prorogato fino a 30 giorni di calendario qualora si debba procedere a un ulteriore esame, ad esempio in caso di consultazione delle autorità centrali.

Tutti questi termini cominciano a decorrere solo quando il fascicolo di candidatura è completo, vale a dire dalla data di ricevimento della domanda di visto e dei documenti giustificativi.

Per le rappresentanze diplomatiche e consolari che hanno un sistema di appuntamenti, il lasso di tempo necessario per essere ricevuti non conta come parte del periodo di trattamento della domanda. In applicazione dell'articolo 7, paragrafo 3, dell'accordo, nel fissare l'appuntamento occorre tenere conto dell'eventuale urgenza dichiarata dal richiedente il visto. Di norma, un appuntamento deve aver luogo entro due settimane da quando viene chiesto (cfr. articolo 6, paragrafo 5, dell'accordo), e un lasso di tempo più lungo deve essere un'eccezione, anche nei periodi di punta. Il comitato misto controllerà attentamente tale questione. Gli Stati membri si impegneranno per garantire che gli appuntamenti su richiesta dei membri delle delegazioni ufficiali dell'Ucraina per presentare le domande presso le rappresentanze diplomatiche e consolari abbiano luogo quanto prima, preferibilmente entro due giorni lavorativi, in casi urgenti, quando l'invito è stato inviato tardi.

La decisione sulla riduzione del termine per decidere su una domanda di visto, secondo la definizione dell'articolo 7, paragrafo 3, dell'accordo, è presa dal funzionario consolare.

2.1.3. *Casi eccezionali di proroga del visto.*

Ai sensi dell'articolo 9 dell'accordo:

> «Qualora, per motivi di forza maggiore, i cittadini ucraini non possano uscire dal territorio degli Stati membri entro il termine stabilito nel visto, il visto è prorogato senza spese conformemente alla normativa dello Stato ospitante per il tempo necessario a ritornare nello Stato di residenza.».

Per quanto riguarda la possibilità di prorogare la validità del visto in casi di forza maggiore, ad esempio ricovero in ospedale per ragioni impreviste/malattia improvvisa/incidente, se il titolare del visto non può lasciare il territorio dello Stato membro entro la data indicata sul visto, si applicano le disposizioni dell'articolo 33, paragrafo 1, del codice dei visti nella misura in cui sono compatibili con l'accordo (ad esempio, il visto prorogato rimane un visto uniforme che dà accesso al territorio di tutti gli Stati membri Schengen per i quali il visto era valido al momento del rilascio). Ai sensi dell'accordo, comunque, nei casi di forza maggiore la proroga del visto è gratuita.

2.2. **Regole applicabili a determinate categorie di richiedenti il visto**

2.2.1. *Documenti giustificativi riguardanti la finalità del viaggio*

Per tutte le categorie di persone elencate all'articolo 4, paragrafo 1, dell'accordo, inclusi gli autotrasportatori che effettuano servizi di trasporto internazionale di merci e passeggeri, per dimostrare la finalità del viaggio sono richiesti solo i documenti giustificativi indicati. Per queste categorie di richiedenti non deve essere chiesto nessun altro documento riguardante la finalità del soggiorno. Come enunciato all'articolo 4, paragrafo 3, dell'accordo, non sono necessari altri inviti, convalide o giustificazioni della finalità del viaggio.

Se, in singoli casi, permangono dubbi quanto al reale scopo dello spostamento, il richiedente il visto sarà convocato per un colloquio (supplementare) approfondito presso l'ambasciata/il consolato, dove potrà essere interrogato sull'effettiva finalità della sua visita o sulla sua intenzione di lasciare il territorio degli Stati membri (cfr. l'articolo 21, paragrafo 8, del codice dei visti). In tali singoli casi, documenti supplementari possono essere forniti dal richiedente il visto oppure eccezionalmente chiesti dal funzionario consolare. Il comitato misto controllerà attentamente la questione.

Per le categorie di persone non menzionate all'articolo 4, paragrafo 1, dell'accordo in materia di documentazione comprovante la finalità del viaggio continuano ad applicarsi le norme attuali. Lo stesso vale per quanto riguarda il consenso dei genitori ai viaggi dei minori di età inferiore ai 18 anni.

Le questioni non contemplate dalle disposizioni dell'accordo, quali il riconoscimento dei documenti di viaggio, l'assicurazione sanitaria di viaggio, le garanzie di attendibilità circa il ritorno e i mezzi di sostentamento sufficienti, sono disciplinate dalle norme Schengen o dal diritto nazionale (cfr. I.1.2).

Conformemente alla dichiarazione dell'Unione europea sulla documentazione da allegare alla domanda di visto per soggiorni di breve durata, acclusa all'accordo di modifica, «L'Unione europea stila un elenco armonizzato di documenti giustificativi, conformemente all'articolo 48, paragrafo 1, lettera a), del codice dei visti, per garantire che i richiedenti ucraini siano tenuti a presentare, in linea di principio, la stessa documentazione giustificativa». I consolati degli Stati membri, agendo nell'ambito della cooperazione locale Schengen, sono tenuti a garantire che i richiedenti il visto ucraini ricevano informazioni di base coerenti e uniformi e che vengano chiesti loro, in linea di principio, gli stessi documenti giustificativi indipendentemente dal consolato dello Stato membro presso il quale fanno domanda.

In linea di principio, contestualmente alla domanda di visto sarà presentata la richiesta originale o il certificato di cui all'articolo 4, paragrafo 1, dell'accordo. Il consolato può comunque cominciare a trattare la domanda con un duplicato o con una copia della richiesta o del certificato. Il consolato può tuttavia richiedere il documento originale in caso di una prima domanda e potrà farlo anche in singoli casi qualora sorgano dubbi.

Poiché l'elenco di autorità figurante in appresso contiene talvolta anche il nome della persona che può firmare le richieste/i certificati rilevanti, in caso di sostituzioni di tali persone le autorità ucraine devono informare la cooperazione locale Schengen.

L'articolo 4 dell'accordo recita quanto segue:

«1. Per le seguenti categorie di cittadini ucraini, i documenti di seguito indicati sono sufficienti per giustificare la finalità del viaggio nel territorio dell'altra parte:

a) per i membri di delegazioni ufficiali che, su invito ufficiale rivolto all'Ucraina, partecipano a riunioni, consultazioni, negoziati o programmi di scambio, o a eventi organizzati nel territorio di uno Stato membro da organizzazioni intergovernative:

— una lettera emessa da un'autorità ucraina attestante che il richiedente è membro della sua delegazione in viaggio nel territorio dell'altra parte per partecipare ai suddetti eventi, corredata di una copia dell'invito ufficiale;».

Nella lettera emessa dall'autorità competente deve essere indicato il nome del richiedente, a conferma del fatto che la persona fa parte della delegazione in viaggio nel territorio dell'altra parte per partecipare alla riunione ufficiale. Il nome del richiedente non deve necessariamente figurare anche sull'invito ufficiale a partecipare alla riunione, benché ciò possa avvenire quando l'invito ufficiale è rivolto a una specifica persona.

Tale disposizione si applica ai membri delle delegazioni ufficiali indipendentemente dal tipo di passaporto (passaporto di servizio od ordinario non biometrico) di cui sono titolari.

«b) per gli imprenditori e i rappresentanti di organizzazioni di categoria:

— una richiesta scritta della persona giuridica o della società ospitante, di un loro ufficio o di una loro filiale, delle autorità statali e locali degli Stati membri, dei comitati organizzatori di fiere, conferenze e convegni commerciali e industriali nel territorio degli Stati membri;

c) per gli autotrasportatori che effettuano servizi di trasporto internazionale di merci e passeggeri nel territorio degli Stati membri con veicoli immatricolati in Ucraina:

— una richiesta scritta dell'associazione nazionale dei trasportatori ucraini relativa a un trasporto internazionale su strada, indicante la finalità, la durata, la destinazione o le destinazioni e la frequenza dei viaggi;».

In appresso figura l'elenco delle autorità competenti per il trasporto internazionale su strada, e responsabili dell'indicazione della finalità, della durata, della o delle destinazioni e della frequenza dei viaggi degli autotrasportatori che effettuano servizi di trasporto internazionale di merci e passeggeri nel territorio degli Stati membri con veicoli immatricolati in Ucraina:

1. Association of International Road Carriers of Ukraine («Associazione dei trasportatori su strada internazionali dell'Ucraina») (AsMAP/«АсМАП»)

   Indirizzo postale dell'AsMAP:

   11, Shorsa str.

   Kiev, 03150, Ucraina

   Funzionari autorizzati a firmare le richieste:

   Kostiuchenko Leonid — presidente dell'AsMAP dell'Ucraina;

   Dokil' Leonid — Vicepresidente dell'AsMAP dell'Ucraina;

   Kuchynskiy Yurii — Vicepresidente dell'AsMAP dell'Ucraina.

2. State Enterprise «Service on International Road Carriages» (Impresa statale «Servizio di trasporto su strada internazionale») (SE «SIRC»)

   Indirizzo postale della SE «SIRC»:

   57, av. Nauka

   Kiev, 03083, Ucraina

   Tel. +38 044 524 21 01

   Fax +38 044 524 00 70

   Funzionari autorizzati a firmare le richieste:

   Tkachenko Anatolij — Direttore della SE «SIRC»;

   Neronov Oleksandr — Primo vicedirettore della SE «SIRC».

3. Ukrainian Road Transport and Logistics Union («Unione per il trasporto su strada e la logistica»)

   Indirizzo postale:

   28, Predslavinska str.

   Kiev, 03150, Ucraina

   Tel./fax +38 044 528 71 30/+38 044 528 71 46/+38 044 529 44 40

   Funzionario autorizzato a firmare le richieste:

   Lypovskiy Vitalij — presidente dell'Unione

4. All-Ukrainian Association of Automobile Carriers (AAAC) («Всеукраїнська асоціація автомобільних перевізників») (Associazione pan-ucraina dei trasportatori automobilistici)

   Indirizzo postale dell'AAAC:

   139, Velyka Vasylkivska str.

   Kiev, 03150, Ucraina

   Tel./fax +38044-538-75-05, +38044-529-25-21

   Funzionari autorizzati a firmare le richieste:

   Reva Vitalii (Віталій Рева) — presidente dell'AAAC

   Glavatskyi Petro (Петро Главатський) — Vicepresidente dell'AAAC

   e-mail: vaap@i.com.ua

5. All-Ukrainian Association of Automobile Carriers (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   Indirizzo postale dell'AAAC:

   3, Rayisy Okipnoyi str.

   Kiev, 02002, Ucraina

   Tel./fax +38044-517-44-31, +38044-516-47-26

   Funzionari autorizzati a firmare le richieste:

   Vakulenko Volodymyr (Вакуленко Володимир Михайлович) — Vicepresidente dell'AAAC

6. Ukrainian State Enterprise «Ukrinteravtoservice» (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів «Укрінтеравтосервіс») (Impresa statale ucraina «Ukrinteravtoservice»)

   Indirizzo postale dell'impresa statale ucraina «Ukrinteravtoservice»:

   57, av. Nauky

   Kiev, 03083, Ucraina

   Funzionari autorizzati a firmare le richieste:

   Dobrohod Serhii (Доброход Сергій Олександрович) — Direttore generale dell'impresa statale ucraina «Ukrinteravtoservice» (tel. +38 044 524-09-99; cell. +38 050 463-89-32);

   Kubalska Svitlana (Кубальська Світлана Сергіївна) — Vicedirettore generale dell'impresa statale ucraina «Ukrinteravtoservice» (tel. +38 044 524-09-99; cell. +38 050 550-82-62)

Tenuto conto degli attuali problemi con tale categoria di richiedenti il visto, il comitato misto controllerà attentamente l'attuazione di detta disposizione.

«d) per il personale di carrozza, di locomotiva o addetto ai vagoni frigoriferi di treni internazionali che viaggiano nei territori degli Stati membri:

— su richiesta scritta della società ferroviaria competente dell'Ucraina, indicante la finalità, la durata e la frequenza dei viaggi;».

L'autorità competente ucraina nel campo del trasporto ferroviario è l'Amministrazione statale del trasporto ferroviario dell'Ucraina («Ukrzaliznytsia»/«Укрзалізниця»).

Indirizzo postale di Ukrzaliznytsia:

5-7 Tverskaya str.
Kiev, 03680, Ucraina

Sulla base della ripartizione delle competenze in seno alla direzione di Ukrzaliznytsia, i funzionari responsabili di fornire le informazioni riguardanti la finalità, la durata e la frequenza dei viaggi del personale di carrozza, di locomotiva o addetto ai vagoni frigoriferi di treni internazionali che viaggiano nei territori degli Stati membri sono i seguenti:

Bolobolin Serhii (Болоболін Сергій Петрович) — Primo direttore generale di Ukrzaliznytsia (tel. +38 044 465 00 10);

Serhiyenko Mykola (Сергієнко Микола Іванович) — Primo vicedirettore generale di Ukrzaliznytsia (tel. +38 044 465 00 01);

Zhurakivskyy Vitaliy (Жураківський Віталій Олександрович) — Primo vicedirettore generale di Ukrzaliznytsia (tel. +38 044 465 00 41);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) — Vicedirettore generale di Ukrzaliznytsia (tel. +38 044 465 00 14);

Naumenko Petro (Науменко Петро Петрович) — Vicedirettore generale di Ukrzaliznytsia (tel. +38 044 465 00 12);

Chekalov Pavlo (Чекалов Павло Леонтійович) — Vicedirettore generale di Ukrzaliznytsia (tel. +38 044 465 00 13);

Matviiv Igor — Capo del Dipartimento di relazioni internazionali di Ukrzaliznytsia (tel. +38 044 465 04 25).

«e) per i giornalisti e per il personale tecnico che li accompagna a titolo professionale:

— un certificato o altro documento rilasciato da un'associazione di categoria o dal datore di lavoro del richiedente, in cui si attesti che l'interessato è un giornalista qualificato, e in cui si dichiari che la finalità del viaggio è la realizzazione di un lavoro giornalistico, o in cui si attesti che l'interessato fa parte del personale tecnico che accompagna il giornalista a titolo professionale».

Questa categoria non contempla i giornalisti free-lance.

Deve essere presentato il certificato o il documento attestante che il richiedente è un giornalista professionista, e il documento originale rilasciato dal datore di lavoro in cui si dichiari che la finalità del viaggio è la realizzazione di un lavoro giornalistico o in cui si attesti che l'interessato fa parte del personale tecnico che accompagna il giornalista a titolo professionale.

L'associazione di categoria ucraina competente ad attestare che l'interessato è un giornalista qualificato è la seguente:

1. National Union of Journalists of Ukraine (NUJU) («Національна спілка журналістів України», НСЖУ) (Unione nazionale dei giornalisti dell'Ucraina).

   La NUJU rilascia agli operatori dei media le tessere nazionali di giornalista e le tessere di giornalista internazionali conformi al modello standard della Federazione internazionale dei giornalisti.

   Indirizzo postale della NUJU:

   27-a Khreschatyk str.

   Kiev, 01001, Ucraina

   Persona autorizzata della NUJU:

   Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) — Capo della NUJU

   Tel/Fax +38044-234-20-96; +38044-234-49-60; +38044-234-52-09

   e-mail: spilka@nsju.org; admin@nsju.org.

2. Independent MEDIA Union of Ukraine (IMUU) («Незалежна медіа-профспілка України») (Unione dei media indipendenti dell'Ucraina)

   Indirizzo postale dell'IMUU:

   Office 25,

   27 — A, Khreshchatyk Str.,

   Kiev, 01001, Ucraina

   Persone autorizzate:

   Lukanov Yurii (Луканов Юрій Вадимович) — Capo dell'IMUU

   Vynnychuk Oksana (Оксана Винничук) — segretario esecutivo dell'IMUU

   Tel.+ 38 050 356 57 58

   e-mail: secretar@profspilka.org.ua

«f) per i partecipanti ad attività scientifiche, culturali e artistiche, inclusi i programmi di scambi universitari o di altro tipo:

— una richiesta scritta a partecipare a dette attività, rilasciata dall'organizzazione ospitante;

g) per gli studenti di scuole inferiori e superiori, di università o corsi post-universitari e per i docenti accompagnatori che effettuano viaggi di studio o di formazione, anche nell'ambito di programmi di scambio o di altre attività scolastiche/accademiche:

— una richiesta scritta o un certificato di iscrizione dell'università, collegio o scuola ospitante, o una carta dello studente o un certificato attestante i corsi da frequentare;».

La carta dello studente può essere accettata come giustificativo della finalità del viaggio solo se rilasciata dall'università, dal collegio o dalla scuola ospitante in cui avrà luogo lo studio o la formazione.

«h) per i partecipanti a eventi sportivi internazionali e le persone che li accompagnano a titolo professionale:

— una richiesta scritta dell'organizzazione ospitante: autorità competenti, federazioni sportive nazionali e comitati olimpici nazionali degli Stati membri;».

Nell'elenco degli accompagnatori per le manifestazioni sportive internazionali figurano solo le persone che accompagnano gli sportivi a titolo professionale: allenatori, massaggiatori, manager, personale medico e dirigenti dei club sportivi. I tifosi non sarannno considerati accompagnatori.

«i) per i partecipanti a programmi di scambi ufficiali organizzati da città gemellate e da altre entità municipali:

— una richiesta scritta del capo dell'amministrazione/sindaco di tali città o altre entità municipali».

Il capo dell'amministrazione/sindaco della città o altra entità municipale competente a rilasciare la richiesta scritta è il capo dell'amministrazione/sindaco della città ospitante o del comune in cui ha luogo l'attività di gemellaggio. Questa categoria riguarda solo i gemellaggi ufficiali.

«j) per i parenti stretti — coniugi, figli (anche adottivi), genitori (anche tutori), nonni e nipoti — in visita a cittadini dell'Ucraina regolarmente soggiornanti nel territorio degli Stati membri o a cittadini dell'Unione europea residenti nel territorio dello Stato membro di cui hanno la cittadinanza:

— una richiesta scritta della persona ospitante;».

Detto punto disciplina la situazione dei parenti stretti ucraini che si recano in Stati membri in visita a cittadini ucraini regolarmente soggiornanti negli Stati membri o a cittadini dell'Unione europea residenti nel territorio dello Stato membro di cui hanno la cittadinanza.

L'autenticità della firma della persona che invita deve essere comprovata dall'autorità competente conformemente al diritto nazionale del paese di soggiorno o residenza.

Occorre inoltre dimostrare la regolarità del soggiorno della persona che invita e il vincolo familiare: la persona ospitante deve ad esempio presentare, insieme alla richiesta scritta, copia dei documenti che attestino il suo status (come una fotocopia del permesso di soggiorno) e confermino i legami familiari.

Detta disposizione si applica anche ai parenti del personale di rappresentanze diplomatiche o consolari che si recano nel territorio degli Stati membri ai fini di una visita familiare di massimo 90 giorni. In questi casi la persona che invita non deve però fornire la prova della regolarità del soggiorno e del vincolo familiare.

Secondo quanto indica la dichiarazione dell'Unione europea relativa alle semplificazioni per i familiari, acclusa all'accordo di modifica, «[p]er favorire la mobilità di un maggiore numero di persone aventi legami familiari (in particolare sorelle, fratelli e rispettivi figli) con cittadini dell'Ucraina regolarmente soggiornanti nei territori degli Stati membri o con cittadini dell'Unione europea che risiedono nel territorio dello Stato membro di cui hanno la cittadinanza, l'Unione europea invita le rappresentanze consolari degli Stati membri ad avvalersi di tutte le possibilità previste dal codice dei visti per facilitare il rilascio dei visti a questa categoria di persone, in particolare semplificando i documenti giustificativi necessari, concedendo esenzioni dai diritti per il trattamento delle domande ed eventualmente rilasciando visti per ingressi multipli.».

«k) per familiari in visita a cimiteri:

— un documento ufficiale attestante il decesso e il sussistere di un vincolo di parentela o di altro tipo tra il richiedente e la persona sepolta;».

L'accordo non specifica quali autorità del paese debbano rilasciare il sopra indicato documento ufficiale: quelle del paese in cui ha luogo la sepoltura o quelle del paese di residenza della persona che si deve recare alla cerimonia. Dovrebbero poter rilasciare tale documento ufficiale le autorità competenti di entrambi i paesi.

Occorre comunque presentare il sopra indicato documento ufficiale attestante il decesso e il vincolo di parentela o di altro tipo tra il richiedente e il defunto; ad esempio certificato di nascita e/o di matrimonio).

«l) per coloro che visitano cimiteri militari e civili:

— un documento ufficiale attestante la sussistenza e la conservazione della tomba, nonché l'esistenza di un vincolo di parentela o di altro tipo tra il richiedente e la persona sepolta;».

L'accordo non specifica se il sopra indicato documento ufficiale debba essere rilasciato dalle autorità del paese in cui si trova il cimitero o da quelle del paese di residenza della persona che intende visitarlo. Dovrebbero poter rilasciare tale documento ufficiale le autorità competenti di entrambi i paesi.

Occorre comunque presentare il sopra indicato documento ufficiale attestante la sussistenza e la conservazione della tomba, nonché l'esistenza di un vincolo di parentela o di altro tipo tra il richiedente e la persona sepolta.

Conformemente alla dichiarazione della Comunità europea sul rilascio dei visti di breve soggiorno per le visite di cimiteri militari e civili acclusa all'accordo, a chi desidera recarsi in visita a cimiteri militari e civili sarannno rilasciati visti per soggiorni di breve durata validi per un periodo massimo di 14 giorni.

«m) per le persone in visita per ragioni mediche e i necessari accompagnatori:

— un documento ufficiale dell'istituto di cura che conferma la necessità di cure mediche presso tale istituto, la necessità di un accompagnamento e la prova della sufficienza dei mezzi finanziari per pagare le cure mediche;».

Occorrerà presentare il documento ufficiale dell'istituto di cura che conferma la necessità di cure mediche presso quell'istituto e la prova della sufficienza dei mezzi finanziari per pagare il costo delle cure mediche, e che confermi anche la necessità dell'accompagnamento.

«n) per i rappresentanti di organizzazioni della società civile in viaggio a fini di formazione, seminari e conferenze, anche nel quadro di programmi di scambio:

— una richiesta scritta dell'organizzazione ospitante, la conferma che l'interessato rappresenta l'organizzazione della società civile e il certificato di esistenza dell'organizzazione in questione, come risulta dall'apposito registro, rilasciato dall'autorità statale conformemente al diritto nazionale;».

Il documento che attesta la registrazione, in Ucraina, di un'organizzazione della società civile è una lettera rilasciata dal Servizio statale di registrazione dell'Ucraina con informazioni tratte dal registro delle associazioni pubbliche.

«o) per i liberi professionisti che partecipano a fiere, conferenze, convegni, seminari internazionali o altri eventi analoghi organizzati nel territorio degli Stati membri:

— una richiesta scritta dell'organizzazione ospitante che conferma la partecipazione dell'interessato all'evento;

p) per i rappresentanti di comunità religiose:

— una richiesta scritta di una comunità religiosa registrata in Ucraina, indicante la finalità, la durata e la frequenza dei viaggi;».

In Ucraina, il documento attestante la registrazione di una comunità religiosa è un estratto del Registro statale unificato delle persone giuridiche e degli imprenditori indicante che la forma giuridica e organizzativa di una persona giuridica corrisponde a una comunità religiosa.

«q) per i partecipanti a programmi ufficiali di cooperazione transfrontaliera dell'Unione europea, come ad esempio nell'ambito dello strumento europeo di vicinato e partenariato (ENPI):

— una richiesta scritta dell'organizzazione ospitante.».

Importante — L'accordo non crea nessuna nuova norma in materia di responsabilità per le persone fisiche o giuridiche che rilasciano le richieste scritte. In caso di falso rilascio di tali richieste si applicano il diritto dell'UE/i rispettivi diritti nazionali.

2.2.2. *Rilascio di visti per più ingressi*

Qualora il richiedente abbia necessità di recarsi frequentemente o regolarmente nel territorio degli Stati membri, sarannno rilasciati visti per soggiorni di breve durata per più visite, purché la durata totale di tali visite non superi i 90 giorni su un periodo di 180 giorni.

L'articolo 5, paragrafo 1, dell'accordo stabilisce quanto segue:

«1. Le rappresentanze diplomatiche e consolari degli Stati membri rilasciano visti per più ingressi validi cinque anni alle seguenti categorie di persone:

a) membri di governi e parlamenti nazionali e regionali e membri di corti costituzionali o di tribunali di ultimo grado, procuratori nazionali e regionali e loro sostituti, che non siano esenti dall'obbligo di visto in virtù del presente accordo, nell'esercizio delle loro funzioni;

b) membri permanenti di delegazioni ufficiali che, su invito ufficiale rivolto all'Ucraina, devono partecipare regolarmente a riunioni, consultazioni, negoziati o programmi di scambio, o a eventi organizzati nel territorio di uno Stato membro da organizzazioni intergovernative;

c) coniugi e figli (anche adottivi) di età inferiore a ventuno anni o a carico, e genitori (anche tutori) in visita a cittadini dell'Ucraina regolarmente soggiornanti nel territorio degli Stati membri o a cittadini dell'Unione europea che risiedono nel territorio dello Stato membro di cui hanno la cittadinanza;

d) uomini d'affari e rappresentanti delle organizzazioni imprenditoriali che si recano regolarmente nel territorio degli Stati membri;

e) giornalisti e personale tecnico che li accompagna a titolo professionale.

In deroga al primo comma, se la necessità o l'intenzione di viaggiare frequentemente o regolarmente è chiaramente limitata a un periodo più corto, la validità del visto per più ingressi è limitata a tale periodo, in particolare quando

— per le persone di cui alla lettera a), la durata dell'incarico,

— per le persone di cui alla lettera b), la validità dello status di membro permanente di una delegazione ufficiale,

— per le persone di cui alla lettera c), il periodo di validità dell'autorizzazione di soggiorno regolare dei cittadini dell'Ucraina regolarmente soggiornanti nell'Unione europea,

— per le persone di cui alla lettera d), la validità dello status di rappresentante di organizzazione imprenditoriale o del contratto di lavoro,

— per le persone di cui alla lettera e), il contratto di lavoro

è inferiore a cinque anni.».

Per tali categorie di persone, tenuto conto del loro status professionale o del loro legame familiare con un cittadino ucraino regolarmente soggiornante nel territorio degli Stati membri o con un cittadino dell'Unione europea che risiede nel territorio dello Stato membro di cui ha la cittadinanza, è giustificato rilasciare, di norma, visti per più ingressi validi cinque anni. L'espressione «validi fino a cinque anni» contenuta nella versione iniziale dell'accordo, che indicava solo la durata massima, lasciava ai consolati un margine di discrezionalità nel decidere la validità del visto. Tale margine di discrezionalità non esiste più con la nuova formulazione dell'accordo modificato («validi cinque anni»): si stabilisce così che, se il richiedente soddisfa tutte le condizioni di cui all'articolo 5, paragrafo 1, dell'accordo, «le rappresentanze diplomatiche e consolari degli Stati membri rilasciano visti per più ingressi validi cinque anni».

Le persone rientranti nell'ambito d'applicazione dell'articolo 5, paragrafo 1, lettera a), dell'accordo, devono comprovare il loro status professionale e la durata del loro mandato.

Tale disposizione non si applica alle persone rientranti nell'ambito d'applicazione dell'articolo 5, paragrafo 1, lettera a), dell'accordo, esenti dall'obbligo di visto in forza dell'accordo, vale a dire titolari di passaporti diplomatici e passaporti di servizio biometrici.

Le persone rientranti nell'ambito d'applicazione dell'articolo 5, paragrafo 1, lettera b), dell'accordo, devono comprovare il loro status permanente di membro della delegazione e la necessità di partecipare regolarmente a riunioni, consultazioni, negoziati o programmi di scambio.

Le persone rientranti nell'ambito d'applicazione dell'articolo 5, paragrafo 1, lettera c), dell'accordo, devono comprovare la regolarità del soggiorno della persona che invita (cfr. II.2.2.1).

Le persone rientranti nell'ambito d'applicazione dell'articolo 5, paragrafo 1, lettere d) ed e), dell'accordo, devono comprovare il loro status professionale e la durata delle loro attività.

L'articolo 5, paragrafo 2, dell'accordo recita quanto segue:

«2. Le rappresentanze diplomatiche e consolari degli Stati membri rilasciano visti per più ingressi validi un anno alle seguenti categorie di persone, a condizione che nell'anno precedente queste abbiano ottenuto almeno un visto e l'abbiano usato conformemente alla normativa sull'ingresso e il soggiorno nel territorio vigente nello Stato visitato:

a) autotrasportatori che effettuano servizi di trasporto internazionale di merci e passeggeri nel territorio degli Stati membri con veicoli immatricolati in Ucraina;

b) personale di carrozza, di locomotiva o addetto ai vagoni frigoriferi di treni internazionali che viaggiano nei territori degli Stati membri;

c) persone partecipanti ad attività scientifiche, culturali e artistiche, inclusi i programmi di scambi universitari o di altro tipo, che si recano regolarmente nel territorio degli Stati membri;

d) partecipanti a eventi sportivi internazionali e persone che li accompagnano a titolo professionale;

e) partecipanti a programmi di scambio ufficiali organizzati da città gemellate e da altre entità municipali;

f) rappresentanti di organizzazioni della società civile che si recano regolarmente negli Stati membri a fini di formazione, seminari e conferenze, anche nell'ambito di programmi di scambio;

g) partecipanti a programmi ufficiali di cooperazione transfrontaliera dell'Unione europea, come ad esempio lo strumento europeo di vicinato e partenariato (ENPI);

h) studenti di scuole inferiori e superiori che viaggiano regolarmente per studio o per formazione, anche nell'ambito di programmi di scambio;

i) rappresentanti di comunità religiose;

j) liberi professionisti che partecipano a fiere, conferenze, convegni e seminari internazionali o altri eventi analoghi organizzati nel territorio degli Stati membri;

k) persone che hanno necessità di effettuare visite periodiche per motivi di salute e i necessari accompagnatori.

In deroga al primo comma, se la necessità o l'intenzione di viaggiare frequentemente o regolarmente è chiaramente limitata a un periodo più corto, la validità del visto per più ingressi è limitata a tale periodo.».

L'espressione «validi fino a un anno» contenuta nella versione iniziale dell'accordo, che indicava solo la durata massima, lasciava ai consolati un margine di discrezionalità nel decidere la validità del visto. Tale margine di discrezionalità non esiste più con la nuova formulazione dell'accordo modificato («validi un anno»): si stabilisce così che, se il richiedente soddisfa tutte le condizioni di cui all'articolo 5, paragrafo 2, dell'accordo, «le rappresentanze diplomatiche e consolari degli Stati membri rilasciano visti per più ingressi validi un anno». Va notato che i visti per più ingressi validi un anno saranno rilasciati alle sopra indicate categorie di persone se nell'anno precedente (12 mesi) il richiedente il visto ha ottenuto almeno un visto Schengen e l'ha usato conformemente alla normativa sull'ingresso e il soggiorno vigente nello Stato o negli Stati visitati (ad esempio non è rimasto nel territorio degli Stati membri più a lungo di quanto consentito) e se vi sono ragioni per chiedere un visto per più ingressi. Il visto Schengen ottenuto nell'anno precedente può essere stato rilasciato da uno Stato Schengen diverso da quello in cui il richiedente ha chiesto il visto nuovo. Nei casi in cui non sia giustificato rilasciare un visto valido un anno (ad esempio se la durata del programma di scambio è inferiore a un anno o se la persona non ha necessità di viaggiare frequentemente o regolarmente per un anno intero), la validità del visto sarà inferiore a un anno, a condizione che siano soddisfatte le altre condizioni di rilascio.

L'articolo 5, paragrafo 3, dell'accordo recita quanto segue:

«3. Le rappresentanze diplomatiche e consolari degli Stati membri rilasciano visti per più ingressi validi da un minimo di due a un massimo di cinque anni alle categorie di persone di cui al paragrafo 2 del presente articolo, a condizione che nei due anni precedenti queste abbiano utilizzato un visto per più ingressi conformemente alla normativa sull'ingresso e il soggiorno nel territorio vigente nello Stato visitato, e a meno che la necessità o l'intenzione di viaggiare frequentemente o regolarmente non sia chiaramente limitata a un periodo più corto, nel qual caso la validità del visto per più ingressi è limitata a tale periodo.

4. La durata totale del soggiorno nel territorio degli Stati membri delle persone di cui ai paragrafi da 1 a 3 del presente articolo non può essere superiore a 90 giorni per periodi di 180 giorni.».

Alle categorie di cui all'articolo 5, paragrafo 2, dell'accordo sarannno rilasciati visti per più ingressi validi da due a cinque anni massimo a condizione che nei due anni precedenti gli interessati abbiano utilizzato un visto Schengen per più ingressi conformemente alla normativa sull'ingresso e il soggiorno vigente nei territori dello Stato o degli Stati visitati, e che la necessità di viaggiare frequentemente o regolarmente non sia manifestamente limitata a un periodo più breve. Va osservato che un visto valido da due a cinque anni sarà rilasciato solo se nei due anni precedenti il richiedente ha ottenuto due visti validi per un anno — e non meno –, e se ha usato questi visti conformemente alla normativa sull'ingresso e il soggiorno vigente nei territori dello o degli Stati visitati. Il periodo di validità di questi visti, vale a dire da due a cinque anni, sarà deciso dalle rappresentanze diplomatiche e consolari degli Stati membri in base alla valutazione di ciascuna domanda.

Per quanto riguarda la definizione dei criteri di cui all'articolo 5, paragrafo 2, dell'accordo («a condizione […] che sussistano motivi per richiedere un visto per più ingressi»), e di cui all'articolo 5, paragrafo 3, dell'accordo («a condizione che […] i motivi per richiedere un visto per più ingressi siano ancora validi»), si applicano i criteri stabiliti per il rilascio di questi tipi di visti dall'articolo 24, paragrafo 2, lettera a), del codice dei visti, vale a dire la necessità dell'interessato di viaggiare frequentemente in uno o più Stati membri, ad esempio per affari.

Se il richiedente non ha utilizzato un visto precedente non vi è obbligo di rilasciare un visto per più ingressi. Tale visto può essere tuttavia emesso se il mancato utilizzo del visto precedente è dovuto a circostanze indipendenti dalla volontà dell'interessato, ad esempio una lunga assenza dal lavoro di autotrasportatore per malattia.

Per quanto riguarda i documenti giustificativi della finalità del viaggio ai fini del rilascio dei visti per più ingressi per le categorie di cui all'articolo 5 dell'accordo, cfr. II.2.2.1.

2.2.3. *Titolari di passaporti diplomatici e di servizio*

L'articolo 10 dell'accordo stabilisce quanto segue:

> «1. I cittadini ucraini titolari di passaporto diplomatico valido possono entrare nei territori degli Stati membri, uscirne e transitarvi senza visto.
>
> 2. I cittadini dell'Ucraina che siano titolari di un passaporto di servizio biometrico valido possono entrare nei territori degli Stati membri, uscirne e transitarvi senza visto.
>
> 3. Le persone di cui ai paragrafi 1 e 2 del presente articolo possono soggiornare nei territori degli Stati membri per un periodo massimo di 90 giorni per periodi di 180 giorni.».

Gli accordi o le intese bilaterali esistenti che prevedono l'esenzione dal visto per i titolari di passaporti di servizio non biometrici continueranno ad applicarsi a meno che non siano denunciati o sospesi (cfr. I.1.6).

L'assegnazione dei diplomatici negli Stati membri non è disciplinata dall'accordo. Si applica l'abituale procedura di accreditamento.

III. STATISTICHE

Per consentire al comitato misto di controllare efficacemente l'accordo, ogni sei mesi le rappresentanze diplomatiche e consolari degli Stati membri devono presentare alla Commissione statistiche riguardanti in particolare, se possibile, e con una ripartizione dei dati per mesi:

— i tipi di visti rilasciati alle varie categorie contemplate dall'accordo;

— il numero di visti rifiutati per le varie categorie di persone contemplate dall'accordo;

— le percentuali di richiedenti, per categorie di persone, convocati a un colloquio;

— il numero di visti per più ingressi validi cinque anni rilasciati ai cittadini ucraini (per paese);

— la percentuale di visti rilasciati gratuitamente alle diverse categorie di persone contemplate dall'accordo.

DECISIONE (PESC) 2015/439 DEL CONSIGLIO

del 16 marzo 2015

che proroga il mandato del rappresentante speciale dell'Unione europea per il Sahel

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 33 e l'articolo 31, paragrafo 2,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 18 marzo 2013 il Consiglio ha adottato la decisione 2013/133/PESC ([1]) che nomina il sig. Michel Dominique REVEYRAND — DE MENTHON rappresentante speciale dell'Unione europea (RSUE) per il Sahel. Il mandato dell'RSUE è stato prorogato dalla decisione 2014/130/PESC del Consiglio ([2]) e scade il 28 febbraio 2015.

(2) Il mandato dell'RSUE dovrebbe essere prorogato di altri otto mesi.

(3) L'RSUE espleterà il suo mandato nell'ambito di una situazione che potrebbe deteriorarsi e compromettere il raggiungimento degli obiettivi dell'azione esterna dell'Unione enunciati nell'articolo 21 del trattato,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Rappresentante speciale dell'Unione europea

1. Il mandato del sig. Michel Dominique REVEYRAND — DE MENTHON quale RSUE per il Sahel è prorogato fino al 31 ottobre 2015. Il mandato dell'RSUE può terminare anticipatamente, se il Consiglio decide in tal senso, su proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (AR).

2. Ai fini del mandato dell'RSUE, per Sahel si intende l'area che costituisce l'obiettivo principale della strategia dell'UE per la sicurezza e lo sviluppo nel Sahel («strategia»), vale a dire il Burkina Faso, il Ciad, il Mali, la Mauritania e il Niger. Per quanto riguarda le questioni aventi implicazioni regionali più vaste, l'RSUE avvia un dialogo, se del caso, con altri paesi ed entità regionali o internazionali oltre il Sahel, come pure l'Africa occidentale e il Golfo di Guinea.

3. In considerazione della necessità di un approccio regionale alle sfide interconnesse che caratterizzano la regione, l'RSUE per il Sahel opera in stretta consultazione con altri RSUE pertinenti, tra cui l'RSUE per la regione del Mediterraneo meridionale, l'RSUE per i diritti umani e l'RSUE presso l'Unione africana.

Articolo 2

Obiettivi politici

1. Il mandato dell'RSUE si basa sull'obiettivo politico dell'Unione in relazione al Sahel di contribuire attivamente agli sforzi regionali e internazionali volti a raggiungere una pace duratura, la sicurezza e lo sviluppo nella regione. Inoltre, l'RSUE punta a rafforzare la qualità, l'intensità e l'impatto degli svariati aspetti dell'impegno dell'Unione nel Sahel.

2. L'RSUE contribuisce a sviluppare e attuare l'approccio dell'Unione, che ingloba tutti gli aspetti dell'azione dell'Unione, in particolare negli ambiti della politica, della sicurezza e dello sviluppo, compresa la strategia, nonché a coordinare tutti gli strumenti pertinenti per le azioni dell'Unione.

3. La priorità iniziale è data al Mali e alla sua stabilizzazione a lungo termine e alle dimensioni regionali del conflitto in questo paese.

([1]) Decisione 2013/133/PESC del Consiglio, del 18 marzo 2013, che nomina il rappresentante speciale dell'Unione europea per il Sahel (GU L 75 del 19.3.2013, pag. 29).

([2]) Decisione 2014/130/PESC del Consiglio, del 10 marzo 2014, che proroga il mandato del rappresentante speciale dell'Unione europea per il Sahel (GU L 71 del 12.3.2014, pag. 14).

4. Riguardo al Mali, gli obiettivi politici dell'Unione intendono promuovere, mediante l'uso coordinato ed effettivo di tutti i propri strumenti, il ritorno per il Mali e il suo popolo a un contesto di pace, riconciliazione, sicurezza e sviluppo. Particolare attenzione dovrebbe essere prestata anche a Burkina Faso e Niger, in particolare nella prospettiva di elezioni in questi paesi.

Articolo 3

Mandato

1. Al fine di realizzare gli obiettivi politici dell'Unione relativi al Sahel, l'RSUE ha il mandato di:

a) contribuire attivamente all'attuazione, al coordinamento e all'ulteriore sviluppo dell'approccio globale dell'Unione alla crisi regionale, in base alla sua strategia, con l'obiettivo di rafforzare la coerenza e l'efficienza globali delle attività dell'Unione nel Sahel, in particolare in Mali;

b) avviare un dialogo con tutti i soggetti interessati della regione, governi, autorità regionali, organizzazioni regionali e internazionali, società civile e diaspore, nell'intento di promuovere gli obiettivi dell'Unione e contribuire a una migliore comprensione del ruolo dell'Unione nel Sahel;

c) rappresentare l'Unione nei pertinenti consessi internazionali e regionali, tra cui il gruppo di sostegno e di monitoraggio sulla situazione in Mali, e assicurare la visibilità del sostegno dell'Unione alla gestione delle crisi e alla prevenzione dei conflitti, comprese la missione militare dell'Unione europea volta a contribuire alla formazione delle forze armate maliane (EUTM Mali) e la missione PSDC dell'Unione europea in Niger (EUCAP Sahel Niger);

d) mantenere una stretta cooperazione con le Nazioni Unite (ONU), in particolare il rappresentante speciale del segretario generale per l'Africa occidentale e il rappresentante speciale del segretario generale per il Mali, con l'Unione Africana (UA), in particolare l'alto rappresentante dell'UA per il Mali e il Sahel, con la Comunità economica degli Stati dell'Africa occidentale (ECOWAS) e con gli altri soggetti interessati nazionali, regionali e internazionali più importanti, inclusi altri inviati speciali per il Sahel, nonché con gli organismi pertinenti nella zona del Maghreb;

e) seguire da vicino le dimensioni regionale e transfrontaliera della crisi, compresi il terrorismo, la criminalità organizzata, il contrabbando di armi, la tratta degli esseri umani, il traffico di stupefacenti, i flussi di rifugiati e migratori e i correlati flussi finanziari; in stretta collaborazione con il coordinatore antiterrorismo dell'UE, contribuire all'ulteriore attuazione della strategia antiterrorismo dell'UE;

f) mantenere contatti politici regolari ad alto livello con i paesi della regione interessati da terrorismo e criminalità internazionale, al fine di garantire un approccio coerente e globale e assicurare il ruolo chiave dell'Unione negli sforzi internazionali volti a combattere il terrorismo e la criminalità internazionale. Ciò include il sostegno attivo dell'Unione allo sviluppo di capacità regionali nel settore della sicurezza e assicurare che le cause profonde del terrorismo e della criminalità internazionale nel Sahel siano affrontate in modo adeguato;

g) seguire da vicino le conseguenze politiche e di sicurezza delle crisi umanitarie nella regione;

h) per quanto riguarda il Mali, contribuire agli sforzi regionali e internazionali intesi a favorire la risoluzione della crisi in Mali, in particolare un completo ritorno alla normalità costituzionale e alla governance nell'intero territorio e un dialogo nazionale credibile e inclusivo che porti a una soluzione politica sostenibile;

i) promuovere lo sviluppo delle istituzioni, la riforma del settore della sicurezza e la costruzione della pace e la riconciliazione a lungo termine in Mali;

j) contribuire, in cooperazione con l'RSUE per i diritti umani, all'attuazione della politica dell'Unione in materia di diritti umani nella regione, compresi gli orientamenti dell'UE sui diritti umani, in particolare gli orientamenti dell'UE sui bambini e i conflitti armati nonché in materia di violenza contro le donne e le ragazze e di lotta contro tutte le forme di discriminazione nei loro confronti, così come della politica dell'Unione in materia di donne, pace e sicurezza, anche monitorando e relazionando sugli sviluppi nonché formulando raccomandazioni a tale riguardo, e mantenere contatti regolari con le autorità pertinenti in Mali e nella regione, l'ufficio del procuratore della Corte penale internazionale, l'ufficio dell'alto commissario per i diritti umani e i difensori dei diritti umani e gli osservatori nella regione;

k) vigilare e riferire sul rispetto delle pertinenti risoluzioni del Consiglio di sicurezza dell'ONU (UNSCR), in particolare le UNSCR 2056 (2012), 2071 (2012), 2085 (2012) e 2100 (2013).

2. Ai fini dell'espletamento del suo mandato, l'RSUE tra l'altro:

a) fornisce consulenza e riferisce, se del caso, in merito alla formulazione delle posizioni dell'Unione nei consessi regionali e internazionali al fine di promuovere e consolidare in modo proattivo l'approccio globale dell'Unione alla crisi nel Sahel;

b) mantiene una visione globale di tutte le attività dell'Unione e collabora strettamente con le pertinenti delegazioni dell'Unione.

Articolo 4

Esecuzione del mandato

1. L'RSUE è responsabile dell'esecuzione del mandato, sotto l'autorità dell'AR.

2. Il comitato politico e di sicurezza (CPS) è un interlocutore privilegiato dell'RSUE e ne costituisce il principale punto di contatto con il Consiglio. Il CPS fornisce all'RSUE un orientamento strategico e una direzione politica nell'ambito del mandato, fatte salve le competenze dell'AR.

3. L'RSUE opera in stretto coordinamento con il servizio europeo per l'azione esterna (SEAE) e i suoi servizi competenti, in particolare con il coordinatore per il Sahel.

Articolo 5

Finanziamento

1. L'importo di riferimento finanziario destinato a coprire le spese connesse con il mandato dell'RSUE nel periodo dal 1º marzo 2015 al 31 ottobre 2015 è pari a 900 000 EUR.

2. Le spese sono gestite nel rispetto delle procedure e delle norme applicabili al bilancio generale dell'Unione.

3. La gestione delle spese è oggetto di un contratto fra l'RSUE e la Commissione. L'RSUE è responsabile dinanzi alla Commissione di tutte le spese.

Articolo 6

Costituzione e composizione della squadra

1. Nei limiti del mandato dell'RSUE e dei corrispondenti mezzi finanziari messi a disposizione, l'RSUE è responsabile della costituzione della sua squadra. La squadra dispone delle competenze necessarie su problemi politici e di sicurezza specifici, secondo le esigenze del mandato. L'RSUE informa senza indugio il Consiglio e la Commissione della composizione della squadra.

2. Gli Stati membri, le istituzioni dell'Unione e il SEAE possono proporre il distacco di personale presso l'RSUE. La retribuzione del personale distaccato presso l'RSUE è a carico dello Stato membro o dell'istituzione dell'Unione in questione o del SEAE. Anche gli esperti distaccati dagli Stati membri presso le istituzioni dell'Unione o il SEAE possono essere assegnati all'RSUE. Il personale internazionale a contratto deve avere la cittadinanza di uno Stato membro.

3. Ciascun membro del personale distaccato resta alle dipendenze amministrative dello Stato membro o dell'istituzione dell'Unione che l'ha distaccato ovvero del SEAE e assolve i propri compiti e agisce nell'interesse del mandato dell'RSUE.

4. Il personale dell'RSUE è ubicato presso i competenti uffici del SEAE o le delegazioni dell'Unione per assicurare la coerenza e la corrispondenza delle loro rispettive attività.

Articolo 7

Privilegi e immunità dell'RSUE e del personale dell'RSUE

I privilegi, le immunità e le altre garanzie necessarie per il compimento e il regolare svolgimento della missione dell'RSUE e del suo personale sono convenuti con i paesi ospitanti, a seconda dei casi. Gli Stati membri e il SEAE forniscono tutto il sostegno necessario a tale scopo.

Articolo 8

Sicurezza delle informazioni classificate UE

L'RSUE e i membri della sua squadra rispettano i principi e le norme minime di sicurezza fissati dalla decisione 2013/488/UE del Consiglio ([1]).

([1]) Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).

Articolo 9

Accesso alle informazioni e supporto logistico

1. Gli Stati membri, la Commissione, il SEAE e il segretariato generale del Consiglio assicurano che l'RSUE abbia accesso a ogni pertinente informazione.

2. Le delegazioni e/o gli Stati membri dell'Unione, a seconda dei casi, forniscono il supporto logistico nella regione.

Articolo 10

Sicurezza

Conformemente alla politica dell'Unione in materia di sicurezza del personale schierato al di fuori dell'Unione nell'ambito di una capacità operativa ai sensi del titolo V del trattato, l'RSUE adotta tutte le misure ragionevolmente praticabili, conformemente al suo mandato e in funzione della situazione di sicurezza nell'area geografica di competenza, per garantire la sicurezza di tutto il personale sotto la sua diretta autorità, in particolare:

a) stabilendo un piano di sicurezza specifico, basato su orientamenti forniti dal SEAE, che contempli le misure di sicurezza fisiche, organizzative e procedurali specifiche che regolano la gestione della sicurezza dei movimenti del personale verso l'area geografica e al suo interno, nonché la gestione degli incidenti di sicurezza, e un piano di emergenza e di evacuazione della missione;

b) provvedendo affinché tutto il personale schierato al di fuori dell'Unione abbia una copertura assicurativa contro i rischi gravi, tenuto conto della situazione nell'area geografica;

c) assicurando che tutti i membri della squadra schierati al di fuori dell'Unione, compreso il personale assunto a livello locale, ricevano un'adeguata formazione in materia di sicurezza, prima o al momento dell'arrivo nell'area geografica, sulla base dei livelli di rischio assegnati a tale area;

d) assicurando che siano attuate tutte le raccomandazioni formulate di comune accordo in seguito a valutazioni periodiche della sicurezza e presentando al Consiglio, all'AR e alla Commissione relazioni scritte sull'attuazione di tali raccomandazioni e su altre questioni di sicurezza nell'ambito della relazione sui progressi compiuti e della relazione di esecuzione del mandato.

Articolo 11

Relazioni

1. L'RSUE riferisce periodicamente all'AR e al CPS. Se del caso, l'RSUE riferisce anche ai gruppi di lavoro del Consiglio. Le relazioni periodiche sono diffuse mediante la rete COREU. L'RSUE può presentare relazioni al Consiglio «Affari esteri». Ai sensi dell'articolo 36 del trattato, l'RSUE può essere associato all'informazione del Parlamento europeo.

2. L'RSUE riferisce sul modo migliore di condurre le iniziative dell'Unione, quali il contributo dell'Unione alle riforme, compresi gli aspetti politici dei progetti di sviluppo pertinenti dell'Unione, in coordinamento con le delegazioni dell'Unione nella regione.

Articolo 12

Coordinamento con altri attori dell'Unione

1. Nell'ambito della strategia, l'RSUE contribuisce all'unità, alla coerenza e all'efficacia dell'azione politica e diplomatica dell'Unione e concorre ad assicurare che tutti gli strumenti dell'Unione e le azioni degli Stati membri siano impiegati in un quadro coerente ai fini del raggiungimento degli obiettivi politici dell'Unione.

2. Le attività dell'RSUE sono coordinate con quelle delle delegazioni dell'Unione e della Commissione e con quelle degli altri RSUE attivi nella regione. L'RSUE informa regolarmente le missioni degli Stati membri e le delegazioni dell'Unione nella regione.

3. Sul campo sono mantenuti stretti contatti con i capi delle delegazioni dell'Unione e i capimissione degli Stati membri. L'RSUE, in stretto coordinamento con le delegazioni pertinenti dell'Unione, fornisce orientamenti politici a livello locale ai capi delle missioni EUCAP Sahel Niger ed EUCAP Sahel Mali e al comandante della missione EUTM Mali. Se necessario, l'RSUE, il comandante della missione EUTM Mali e il comandante civile dell'operazione di EUCAP Sahel Niger ed EUCAP Sahel Mali si consultano reciprocamente.

Articolo 13

Riesame

L'attuazione della presente decisione e la coerenza della stessa con altri contributi dell'Unione nella regione sono riesaminate periodicamente. L'RSUE presenta al Consiglio, all'AR e alla Commissione una relazione esauriente sull'esecuzione del mandato entro la fine di agosto 2015.

Articolo 14

Entrata in vigore

La presente decisione entra in vigore il giorno dell'adozione.

Essa si applica a decorrere dal 1º marzo 2015.

Fatto a Bruxelles, il 16 marzo 2015

Per il Consiglio
Il presidente
F. MOGHERINI

DECISIONE (PESC) 2015/440 DEL CONSIGLIO

del 16 marzo 2015

che proroga il mandato del rappresentante speciale dell'Unione europea per il Corno d'Africa

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 33 e l'articolo 31, paragrafo 2,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) L'8 dicembre 2011 il Consiglio ha adottato la decisione 2011/819/PESC [1] che nomina il sig. Alexander RONDOS rappresentante speciale dell'Unione europea (RSUE) per il Corno d'Africa. Il mandato dell'RSUE scade il 28 febbraio 2015.

(2) Il mandato dell'RSUE dovrebbe essere ulteriormente prorogato fino al 31 ottobre 2015.

(3) L'RSUE espleterà il mandato nell'ambito di una situazione che potrebbe deteriorarsi e compromettere il raggiungimento degli obiettivi dell'azione esterna dell'Unione enunciati nell'articolo 21 del trattato,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Rappresentante speciale dell'Unione europea

Il mandato del sig. Alexander RONDOS quale RSUE per il Corno d'Africa è prorogato fino al 31 ottobre 2015. Il Consiglio può decidere che il mandato dell'RSUE termini anticipatamente, sulla base di una valutazione da parte del comitato politico e di sicurezza (CPS) e di una proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (AR).

Ai fini del mandato dell'RSUE, per Corno d'Africa si intende la Repubblica di Gibuti, lo Stato di Eritrea, la Repubblica federale democratica di Etiopia, la Repubblica del Kenya, la Repubblica federale di Somalia, la Repubblica del Sudan, la Repubblica del Sud Sudan e la Repubblica dell'Uganda. Per quanto riguarda le questioni aventi implicazioni regionali più vaste, l'RSUE avvia un dialogo, se del caso, con paesi ed entità regionali oltre il Corno d'Africa.

Articolo 2

Obiettivi politici

1. Il mandato dell'RSUE si basa sugli obiettivi politici dell'Unione in relazione al Corno d'Africa indicati nel quadro strategico adottato il 14 novembre 2011 e nelle pertinenti conclusioni del Consiglio, vale a dire al fine di contribuire attivamente agli sforzi regionali e internazionali volti a raggiungere una coesistenza pacifica e una pace duratura, la sicurezza e lo sviluppo all'interno e tra i paesi della regione. Inoltre, l'RSUE punta a rafforzare la qualità, l'intensità, l'impatto e la visibilità degli svariati aspetti dell'impegno dell'Unione nel Corno d'Africa.

2. Gli obiettivi politici includono, tra l'altro:

a) la continuazione della stabilizzazione della Somalia, in particolare dal punto di vista della dimensione regionale;

b) la pacifica coesistenza tra il Sudan e il Sud Sudan come due Stati vitali e prosperi con strutture politiche solide e responsabili;

c) la risoluzione degli attuali conflitti e l'evitare potenziali conflitti tra i paesi della regione o all'interno degli stessi;

d) il sostegno alla cooperazione regionale in materia politica, di sicurezza ed economica.

[1] Decisione 2011/819/PESC del Consiglio, dell'8 dicembre 2011, che nomina il rappresentante speciale dell'Unione europea per il Corno d'Africa (GU L 327 del 9.12.2011, pag. 62).

Articolo 3

Mandato

1. Al fine di realizzare gli obiettivi politici dell'Unione relativi al Corno d'Africa, l'RSUE ha il mandato di:

a) avviare un dialogo con tutti i soggetti interessati della regione, governi, autorità regionali, organizzazioni internazionali e regionali, società civile e diaspore, nell'intento di promuovere gli obiettivi dell'Unione, e contribuire a una migliore comprensione del ruolo dell'Unione nella regione;

b) rappresentare l'Unione nei pertinenti consessi internazionali, ove opportuno, e assicurare la visibilità del sostegno dell'Unione alla gestione delle crisi e alla risoluzione e alla prevenzione dei conflitti;

c) incoraggiare e sostenere una cooperazione politica e di sicurezza nonché un'integrazione economica efficaci nella regione mediante il partenariato dell'Unione con l'Unione africana (UA) e le organizzazioni regionali, in particolare l'Autorità intergovernativa per lo sviluppo (IGAD);

d) seguire gli sviluppi politici nella regione e contribuire allo sviluppo delle politiche dell'Unione rivolte alla regione, anche in relazione alla Somalia, al Sudan, al Sud Sudan, alla questione della frontiera tra Etiopia ed Eritrea e all'attuazione dell'accordo di Algeri, all'iniziativa del Bacino del Nilo e ad altre questioni che destano preoccupazioni nella regione e che hanno effetti sulla sicurezza, la stabilità e la prosperità;

e) per quanto riguarda la Somalia, e operando in stretto coordinamento con l'inviato speciale dell'UE per la Somalia e i partner pertinenti a livello regionale e internazionale, incluso il rappresentante speciale del segretario generale delle Nazioni Unite (ONU) per la Somalia e l'UA, contribuire attivamente alle azioni e alle iniziative volte all'ulteriore stabilizzazione della Somalia e alla definizione dei piani post-transizione per tale paese, con particolare attenzione alla promozione di un approccio internazionale coordinato e coerente nei confronti della Somalia, all'instaurazione di relazioni di buon vicinato e al sostegno allo sviluppo del settore della sicurezza in Somalia, anche mediante la missione militare dell'Unione europea volta a contribuire alla formazione delle forze di sicurezza somale (EUTM Somalia), la forza navale diretta dall'Unione europea (EUNAVFOR Atalanta), la missione dell'Unione europea per lo sviluppo delle capacità marittime regionali nel Corno d'Africa (EUCAP Nestor) e il continuo sostegno dell'Unione alla missione dell'Unione Africana in Somalia (AMISOM), in stretta collaborazione con gli Stati membri;

f) per quanto riguardo il Sudan e il Sud Sudan, e in stretta cooperazione con i rispettivi capi delegazione dell'Unione, contribuire alla coerenza e all'efficacia della politica dell'Unione nei confronti del Sudan e del Sud Sudan e sostenere la loro pacifica coesistenza, in particolare tramite l'attuazione degli accordi di Addis Abeba e la risoluzione delle questioni in sospeso successive all'accordo globale di pace, incluse Abyei, soluzioni politiche per i conflitti in corso, segnatamente nel Darfur, negli Stati del Kordofan meridionale e del Nilo azzurro, la costruzione istituzionale nel Sud Sudan e la riconciliazione nazionale. In proposito, l'RSUE contribuisce a un approccio internazionale coerente in stretta cooperazione con l'UA, e, in particolare, il gruppo di attuazione ad alto livello dell'UA per il Sudan (AUHIP), l'ONU e altri soggetti interessati fondamentali sia regionali che internazionali;

g) seguire da vicino le sfide transfrontaliere che riguardano il Corno d'Africa, compresi il terrorismo, la radicalizzazione, la sicurezza marittima e la pirateria, la criminalità organizzata, il contrabbando di armi, i flussi di rifugiati e migratori e le eventuali conseguenze politiche o relative alla sicurezza a seguito di crisi umanitarie;

h) promuovere l'accesso umanitario in tutta la regione;

i) contribuire all'attuazione della decisione 2011/168/PESC del Consiglio ([1]) e della politica dell'Unione in materia di diritti umani, in cooperazione con l'RSUE per i diritti umani, compresi gli orientamenti dell'UE sui diritti umani, in particolare gli orientamenti dell'UE sui bambini e i conflitti armati, nonché gli orientamenti dell'UE in materia di violenza contro le donne e le ragazze e di lotta contro tutte le forme di discriminazione contro di loro, così come della politica dell'Unione in relazione alla risoluzione 1325 (2000) del Consiglio di sicurezza delle Nazioni Unite, anche monitorando e relazionando sugli sviluppi, nonché formulando raccomandazioni a tale riguardo.

2. Ai fini dell'espletamento del mandato, l'RSUE tra l'altro:

a) fornisce consulenza e riferisce, se del caso, in merito alla definizione delle posizioni dell'Unione nei consessi internazionali, al fine di promuovere in modo proattivo un approccio politico coerente dell'Unione nei confronti del Corno d'Africa;

b) mantiene una visione globale di tutte le attività dell'Unione.

([1]) Decisione 2011/168/PESC del Consiglio, del 21 marzo 2011, sulla Corte penale internazionale e che abroga la posizione comune 2003/444/PESC (GU L 76 del 22.3.2011, pag. 56).

Articolo 4

Esecuzione del mandato

1. L'RSUE è responsabile dell'esecuzione del mandato, sotto l'autorità dell'AR.

2. Il CPS è un interlocutore privilegiato dell'RSUE e ne costituisce il principale punto di contatto con il Consiglio. Il CPS fornisce all'RSUE un orientamento strategico e una direzione politica nell'ambito del mandato, fatte salve le competenze dell'AR.

3. L'RSUE opera in stretto coordinamento con il servizio europeo per l'azione esterna (SEAE) e i suoi servizi competenti, le delegazioni dell'Unione nella regione e la Commissione.

Articolo 5

Finanziamento

1. L'importo di riferimento finanziario destinato a coprire le spese connesse con il mandato dell'RSUE nel periodo dal 1º marzo 2015 al 31 ottobre 2015 è pari a 1 770 000 EUR.

2. Le spese sono gestite nel rispetto delle procedure e delle norme applicabili al bilancio generale dell'Unione.

3. La gestione delle spese è oggetto di un contratto fra l'RSUE e la Commissione. L'RSUE è responsabile dinanzi alla Commissione di tutte le spese.

Articolo 6

Costituzione e composizione della squadra

1. Nei limiti del mandato dell'RSUE e dei corrispondenti mezzi finanziari messi a disposizione, l'RSUE è responsabile della costituzione della sua squadra. La squadra dispone delle competenze necessarie su problemi politici e di sicurezza specifici, secondo le esigenze del mandato. L'RSUE informa senza indugio e periodicamente il Consiglio e la Commissione della composizione della squadra.

2. Gli Stati membri, le istituzioni dell'Unione e il SEAE possono proporre il distacco di personale presso l'RSUE. La retribuzione di tale personale distaccato è a carico, rispettivamente, dello Stato membro, dell'istituzione dell'Unione in questione o del SEAE. Anche gli esperti distaccati dagli Stati membri presso le istituzioni dell'Unione o il SEAE possono essere assegnati all'RSUE. Il personale internazionale a contratto deve avere la cittadinanza di uno Stato membro.

3. Ciascun membro del personale distaccato resta alle dipendenze amministrative dello Stato membro o dell'istituzione dell'Unione che l'ha distaccato ovvero del SEAE e assolve i propri compiti e agisce nell'interesse del mandato dell'RSUE.

4. Il personale dell'RSUE è ubicato presso i competenti uffici del SEAE o le delegazioni dell'Unione per contribuire alla coerenza e alla corrispondenza delle loro rispettive attività.

Articolo 7

Privilegi e immunità dell'RSUE e del suo personale

I privilegi, le immunità e le altre garanzie necessarie per il compimento e il regolare svolgimento della missione dell'RSUE e del suo personale sono convenuti con i paesi ospitanti, a seconda dei casi. Gli Stati membri e il SEAE forniscono tutto il sostegno necessario a tale scopo.

Articolo 8

Sicurezza delle informazioni classificate UE

L'RSUE e i membri della sua squadra rispettano i principi e le norme minime di sicurezza fissati dalla decisione 2013/488/UE del Consiglio ([1]).

([1]) Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per la protezione delle informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).

Articolo 9

Accesso alle informazioni e supporto logistico

1. Gli Stati membri, la Commissione, il SEAE e il segretariato generale del Consiglio assicurano che l'RSUE abbia accesso a ogni pertinente informazione.

2. Le delegazioni dell'Unione nella regione e gli Stati membri, a seconda dei casi, forniscono il supporto logistico nella regione stessa.

Articolo 10

Sicurezza

Conformemente alla politica dell'Unione in materia di sicurezza del personale schierato al di fuori dell'Unione nell'ambito di una capacità operativa ai sensi del titolo V del trattato, l'RSUE adotta tutte le misure ragionevolmente praticabili, conformemente al suo mandato e in funzione della situazione di sicurezza nell'area geografica di competenza, per garantire la sicurezza di tutto il personale sotto la diretta autorità dell'RSUE, in particolare:

a) stabilendo un piano di sicurezza specifico della missione, basato su orientamenti forniti dal SEAE, che contempli le misure di sicurezza fisiche, organizzative e procedurali specifiche della missione che regolano la gestione della sicurezza dei movimenti del personale verso la zona della missione e al suo interno, nonché la gestione degli incidenti di sicurezza, e un piano di emergenza e di evacuazione della missione;

b) provvedendo affinché tutto il personale schierato al di fuori dell'Unione abbia una copertura assicurativa contro i rischi gravi, tenuto conto della situazione nella zona della missione;

c) assicurando che tutti i membri della squadra dell'RSUE schierati al di fuori dell'Unione, compreso il personale assunto a livello locale, ricevano un'adeguata formazione su questioni relative alla sicurezza, prima o al momento dell'arrivo nella zona della missione, sulla base dei livelli di rischio assegnati dal SEAE alla zona della missione stessa;

d) assicurando che siano attuate tutte le raccomandazioni formulate di comune accordo in seguito a valutazioni periodiche della sicurezza e presentando al Consiglio, all'AR e alla Commissione relazioni scritte sull'attuazione di tali raccomandazioni e su altre questioni di sicurezza nell'ambito delle relazioni sui progressi compiuti e sull'esecuzione del mandato.

Articolo 11

Relazioni

1. L'RSUE riferisce periodicamente all'AR e al CPS oralmente e per iscritto. Se necessario, riferisce anche ai gruppi di lavoro del Consiglio. Le relazioni periodiche sono diffuse mediante la rete COREU. L'RSUE può presentare relazioni al Consiglio «Affari esteri». Ai sensi dell'articolo 36 del trattato, l'RSUE può essere associato all'informazione del Parlamento europeo.

2. L'RSUE riferisce sul modo migliore di condurre le iniziative dell'Unione, quali il contributo dell'Unione alle riforme, compresi gli aspetti politici dei progetti di sviluppo pertinenti dell'Unione, in coordinamento con le delegazioni dell'Unione nella regione.

Articolo 12

Coordinamento

1. L'RSUE contribuisce all'unità, alla coerenza e all'efficacia delle azioni dell'Unione e concorre ad assicurare che tutti gli strumenti dell'Unione e le azioni degli Stati membri siano impiegati in un quadro coerente ai fini del raggiungimento degli obiettivi politici dell'Unione. Le attività dell'RSUE sono coordinate con quelle delle delegazioni dell'Unione e della Commissione. L'RSUE informa regolarmente le missioni degli Stati membri e le delegazioni dell'Unione nella regione.

2. Sul campo sono mantenuti stretti contatti con i capi delle delegazioni dell'Unione e i capimissione degli Stati membri. Essi si adoperano al massimo per assistere l'RSUE nell'esecuzione del mandato. L'RSUE, in stretto coordinamento con le delegazioni pertinenti dell'Unione, fornisce orientamenti politici a livello locale al comandante della forza EUNAVFOR Atalanta, al comandante della missione dell'UE EUTM Somalia e al capo della missione EUCAP Nestor. Se necessario, l'RSUE, il comandante dell'operazione dell'UE e il comandante civile dell'operazione si consultano reciprocamente.

3. L'RSUE coopera strettamente con le autorità dei paesi interessati, con l'ONU, l'UA, l'IGAD, altri soggetti interessati a livello nazionale, regionale e internazionale, nonché con la società civile nella regione.

Articolo 13

Riesame

L'attuazione della presente decisione e la coerenza della stessa con altri contributi dell'Unione nella regione sono riesaminate periodicamente. L'RSUE presenta al Consiglio, all'AR e alla Commissione una relazione esauriente sull'esecuzione del mandato entro il 31 agosto 2015.

Articolo 14

Entrata in vigore

La presente decisione entra in vigore il giorno dell'adozione.

Essa si applica a decorrere dal 1º marzo 2015.

Fatto a Bruxelles, il 16 marzo 2015

Per il Consiglio
Il presidente
F. MOGHERINI

DECISIONE (PESC) 2015/441 DEL CONSIGLIO

del 16 marzo 2015

che modifica e proroga la decisione 2010/96/PESC, relativa alla missione militare dell'Unione europea volta a contribuire alla formazione delle forze di sicurezza somale

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 42, paragrafo 4, e l'articolo 43, paragrafo 2,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 15 febbraio 2010 il Consiglio ha adottato la decisione 2010/96/PESC ([1]). Il mandato della missione militare dell'UE scade il 31 marzo 2015.

(2) La conferenza di Bruxelles sulla Somalia, tenutasi il 16 settembre 2013, ha fornito la base per il «Patto per la Somalia» e attivato un meccanismo di coordinamento e di titolarità somala con la task force «New Deal» per la Somalia.

(3) In occasione dell'incontro internazionale organizzato congiuntamente dal Regno Unito e dalla Somalia il 18 settembre 2014 a Londra, il governo federale ha delineato il percorso di sviluppo dell'esercito nazionale somalo fino al 2019 messo a punto dal ministero della difesa, nonché le sue necessità immediate.

(4) Alla luce del riesame strategico dell'ottobre 2014, il mandato della missione militare dell'UE dovrebbe essere prorogato fino al 31 dicembre 2016.

(5) A norma dell'articolo 5 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'elaborazione e all'attuazione di decisioni e azioni dell'Unione che hanno implicazioni nel settore della difesa. La Danimarca non partecipa all'attuazione della presente decisione e non contribuisce, pertanto, al finanziamento della presente missione.

(6) È opportuno prorogare ulteriormente la missione militare dell'UE con un mandato adattato,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La decisione 2010/96/PESC è così modificata:

1) all'articolo 1, il paragrafo 2 è sostituito dal seguente:

«2. Allo scopo di conseguire gli obiettivi di cui al paragrafo 1, la missione militare dell'UE è schierata in Somalia sia per contribuire ad un potenziamento istituzionale nel settore della difesa attraverso la consulenza strategica, sia per fornire un sostegno diretto all'esercito nazionale somalo attraverso la formazione, la consulenza e l'accompagnamento. La missione militare dell'UE si tiene inoltre pronta a fornire sostegno, nell'ambito dei suoi mezzi e delle sue capacità, ad altri attori dell'Unione per l'attuazione dei rispettivi mandati nel campo della sicurezza e della difesa in Somalia.»;

2) l'articolo 3 è sostituito dal seguente:

«*Articolo 3*

Designazione della sede del comando della missione

1. Il comando della missione è ubicato in Somalia, presso l'aeroporto internazionale di Mogadiscio a Mogadiscio. Esso svolge le funzioni di comando operativo e di comando della forza.

2. Il comando della missione comprende un ufficio di collegamento e sostegno a Nairobi e una cellula di sostegno a Bruxelles.».

([1]) Decisione 2010/96/PESC del Consiglio, del 15 febbraio 2010, relativa alla missione militare dell'Unione europea volta a contribuire alla formazione delle forze di sicurezza somale (GU L 44 del 19.2.2010, pag. 16).

3) all'articolo 7, il paragrafo 4 è sostituito dal seguente:

«4. La missione militare dell'UE opera, nei limiti dei mezzi e delle capacità di cui dispone, in stretta cooperazione con gli altri attori internazionali nella regione, in particolare le Nazioni Unite e l'AMISOM, in linea con le esigenze concordate del governo federale somalo.»;

4) all'articolo 10 è aggiunto il paragrafo seguente:

«5. L'importo di riferimento finanziario per i costi comuni della missione militare dell'UE per il periodo dal 1º aprile 2015 al 31 dicembre 2016 è pari a 17 507 399 EUR. La percentuale dell'importo di riferimento di cui all'articolo 25, paragrafo 1, di ATHENA è pari al 30 % e la percentuale dell'impegno di cui all'articolo 32, paragrafo 3, di ATHENA è pari al 90 %.»;

5) è inserito l'articolo seguente:

«*Articolo 10* ter

Cellula di progetto

1. La missione militare dell'UE dispone di una cellula di progetto per identificare ed attuare progetti, finanziati dagli Stati membri o da Stati terzi, che siano coerenti con gli obiettivi della missione e contribuiscano alla realizzazione del mandato.

2. Fatto salvo il paragrafo 3, il comandante della missione dell'UE è autorizzato a far ricorso ai contributi finanziari degli Stati membri o di Stati terzi per l'attuazione di progetti individuati come complemento coerente delle altre azioni della missione militare dell'EU. In tal caso il comandante della missione dell'UE conclude un accordo con detti Stati, riguardante in particolare le modalità specifiche concernenti la risposta a qualsiasi azione emanante da terzi riguardante danni subiti a causa di atti od omissioni del comandante della missione dell'UE nell'utilizzo dei fondi messi a sua disposizione da detti Stati.

Né l'Unione né l'AR sono in alcun caso ritenuti responsabili dagli Stati contributori per atti od omissioni del comandante della missione dell'UE nell'utilizzo dei fondi forniti da detti Stati.

3. Il CPS approva l'accettazione dei contributi finanziari alla cellula di progetto da parte di Stati terzi.»;

6) l'articolo 11 è così modificato:

a) al paragrafo 1, la frase introduttiva è sostituita dalla seguente: «L'AR è autorizzato a comunicare agli Stati terzi associati alla presente decisione, secondo necessità e in funzione dei bisogni della missione, le informazioni classificate dell'UE prodotte ai fini della missione, conformemente alla decisione 2013/488/UE del Consiglio (*):

(*) Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle regole di sicurezza per proteggere le informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).»;

b) ai paragrafi 2 e 3, i termini «decisione 2011/292/UE» sono sostituiti dai termini «decisione 2013/488/UE»;

7) all'articolo 12, i paragrafi 2 e 3 sono sostituiti dai seguenti:

«2. Il mandato della missione militare dell'UE termina il 31 dicembre 2016.

3. La presente decisione è abrogata a decorrere dalla data di chiusura della sede del comando dell'UE, dell'ufficio di collegamento e sostegno a Nairobi e della cellula di sostegno a Bruxelles conformemente alla pianificazione approvata per la cessazione della missione militare dell'UE e fatte salve le procedure stabilite in ATHENA relative alle attività di revisione e rendimento dei conti della missione militare dell'UE.».

Articolo 2

La presente decisione entra in vigore il giorno dell'adozione.

Essa si applica a decorrere dal 1º aprile 2015.

Fatto a Bruxelles, il 16 marzo 2015

Per il Consiglio
Il presidente
F. MOGHERINI

DECISIONE (PESC) 2015/442 DEL CONSIGLIO

del 16 marzo 2015

relativa all'avvio di una missione militare consultiva dell'Unione europea in ambito PSDC nella Repubblica centrafricana (EUMAM RCA) e che modifica la decisione (PESC) 2015/78

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare gli articoli 42, paragrafo 4, e 43, paragrafo 2,

vista la decisione 2015/78/PESC del Consiglio, del 19 gennaio 2015, relativa a una missione militare consultiva dell'Unione europea in ambito PSDC nella Repubblica centrafricana (EUMAM RCA) ([1]), in particolare l'articolo 4,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 19 gennaio 2015 il Consiglio ha adottato la decisione 2015/78/PESC.

(2) Il 9 febbraio 2015 il Consiglio ha approvato le regole di ingaggio dell'EUMAM RCA.

(3) Il 6 marzo 2015 il Consiglio ha approvato il piano della missione dell'EUMAM RCA.

(4) L'11 marzo 2015 il comitato politico e di sicurezza ha accolto favorevolmente la lettera del comandante della missione relativa all'avvio dell'EUMAM RCA e ai termini previsti per la dichiarazione di avvio della capacità operativa iniziale dell'EUMAM RCA

(5) L'EUMAM RCA dovrebbe essere avviata il 16 marzo 2015.

(6) A norma dell'articolo 5 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'elaborazione e all'attuazione di decisioni e azioni dell'Unione che hanno implicazioni nel settore della difesa. Di conseguenza, la Danimarca non partecipa all'attuazione della presente decisione e, pertanto, non partecipa al finanziamento della presente missione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La missione militare consultiva dell'Unione europea in ambito PSDC nella Repubblica centrafricana («EUMAM RCA») è avviata il 16 marzo 2015.

Articolo 2

Il comandante della missione dell'UE EUMAM RCA è autorizzato, con effetto immediato, a dare avvio all'esecuzione della missione.

Articolo 3

L'articolo 4, paragrafo 2, della decisione (PESC) 2015/78 è sostituito dal seguente:

«2. L'EUMAM RCA prende avvio con una decisione del Consiglio riguardante la data raccomandata dal comandante della missione, successivamente all'approvazione del piano della missione e, qualora si renda necessario, di regole di ingaggio supplementari.».

([1]) GU L 13 del 20.1.2015, pag. 8.

Articolo 4

La presente decisione entra in vigore il giorno dell'adozione.

Fatto a Bruxelles, il 16 marzo 2015

Per il Consiglio
Il presidente
F. MOGHERINI

DECISIONE (UE, Euratom) 2015/443 DELLA COMMISSIONE

del 13 marzo 2015

sulla sicurezza nella Commissione

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,

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) Obiettivo della sicurezza nella Commissione è consentire all'istituzione di agire in un ambiente sicuro grazie a un approccio coerente, integrato per quanto riguarda la sicurezza, che offra adeguati livelli di protezione a persone, risorse e informazioni in funzione dei rischi identificati, e garantisca una sicurezza efficiente e tempestiva.

(2) La Commissione, come altre istituzione internazionali, è sottoposta a minacce e sfide gravi per la sicurezza, in particolare per quanto riguarda il terrorismo, gli attacchi informatici, lo spionaggio politico e commerciale.

(3) La Commissione europea ha concluso accordi relativi alla sicurezza per le proprie sedi principali con i governi di Belgio, Lussemburgo e Italia [1], che confermano che la Commissione è responsabile della propria sicurezza.

(4) Per assicurare la sicurezza delle persone, delle risorse e delle informazioni, la Commissione può essere tenuta ad adottare misure in settori tutelati dai diritti fondamentali iscritti nella Carta dei diritti fondamentali e nella convenzione europea dei diritti dell'uomo e riconosciuti dalla Corte di giustizia europea.

(5) Tali misure devono essere giustificate dall'importanza degli interessi da tutelare, proporzionate e tali da assicurare il pieno rispetto dei diritti fondamentali, soprattutto quelli relativi alla vita privata e alla protezione dei dati.

(6) Nell'ambito di un sistema ispirato allo Stato di diritto e al rispetto dei diritti fondamentali, la Commissione deve adoperarsi per ottenere un livello di sicurezza del personale, delle risorse e delle informazioni tale da permettere lo svolgimento delle proprie attività operative senza limitare i diritti fondamentali oltre lo stretto necessario.

(7) La sicurezza nella Commissione si basa sui principi di legalità, trasparenza, proporzionalità e responsabilità.

(8) I membri del personale incaricato di prendere misure di sicurezza non devono essere penalizzati a causa delle loro attività se non agiscono al di fuori del loro mandato o in violazione della legge; sotto questo aspetto la presente decisione deve pertanto essere considerata come un'istruzione di servizio ai sensi dello statuto dei funzionari.

(9) La Commissione, con iniziative adeguate, deve stimolare e rafforzare la propria cultura della sicurezza, assicurando una sicurezza più efficiente, migliorandone la gestione e intensificando ulteriormente le reti di connessione e la cooperazione con le autorità competenti a livello internazionale, europeo e nazionale, e migliorando il monitoraggio e il controllo dell'attuazione delle misure di sicurezza.

(10) L'istituzione del Servizio europeo per l'azione esterna (SEAE), organo funzionalmente autonomo dell'Unione, ha avuto un impatto sensibile sugli interessi della Commissione in materia di sicurezza, e richiede pertanto l'elaborazione di norme e procedure di collaborazione nel settore della sicurezza e dell'incolumità tra il SEAE e la Commissione, in particolare per quanto riguarda l'assolvimento dell'obbligo di diligenza nei confronti del personale della Commissione nelle delegazioni dell'Unione.

---

[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.

(11) L'attuazione della politica di sicurezza della Commissione dovrebbe essere coerente con altre procedure e processi interni che possono comportare una componente di sicurezza; tra questi, in particolare, la gestione della continuità operativa volta a tutelare le funzioni essenziali della Commissione in caso di perturbazione delle attività operative, e il processo ARGUS di coordinamento delle crisi multisettoriali.

(12) Fatte salve le misure già in vigore al momento dell'adozione della presente decisione, notificate al garante europeo della protezione dei dati ([1]), le disposizioni nell'ambito della presente decisione che comportano il trattamento di dati personali sono oggetto di norme di attuazione conformemente all'articolo 21, che stabilisce adeguate garanzie a tutela delle persone interessate.

(13) Occorre pertanto che la Commissione riesamini, aggiorni e consolidi la base normativa vigente in materia di sicurezza alla Commissione.

(14) È quindi necessario abrogare la decisione (94) 2129 ([2]) della Commissione,

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

DISPOSIZIONI GENERALI

Articolo 1

Definizioni

Ai fini della presente decisione si intende per:

1) «risorse», tutti i beni mobili e immobili di proprietà o in possesso della Commissione;

2) «servizio della Commissione», le direzioni generali, i servizi della Commissione o il gabinetto di un membro della Commissione;

3) «sistema di comunicazione e informazione» o «CIS», ogni sistema che consente il trattamento delle informazioni in forma elettronica, compreso l'insieme delle risorse necessarie al suo funzionamento, nonché l'infrastruttura, l'organizzazione, il personale e le risorse d'informazione;

4) «controllo dei rischi», le misure di sicurezza presumibilmente in grado di tenere efficacemente sotto controllo un rischio per la sicurezza prevenendolo, attenuandolo, evitandolo o trasferendolo;

5) «situazione di crisi», la circostanza, l'evento, l'incidente, l'emergenza (o una combinazione simultanea o successiva di questi) tale da mettere in pericolo grave o immediato la sicurezza nella Commissione, a prescindere dall'origine;

6) «dati», l'informazione in una forma che ne consente la comunicazione, la registrazione o il trattamento;

7) «membro della Commissione responsabile della sicurezza», il membro della Commissione sotto l'autorità del quale rientra la direzione generale Risorse umane e sicurezza;

8) «dati personali», i dati personali definiti nell'articolo 2, lettera a) del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([3]);

9) «locali», beni immobili o assimilabili di proprietà o in possesso della Commissione;

10) «prevenzione del rischio», le misure di sicurezza che presumibilmente impediscono, ritardano o pongono termine a un rischio per la sicurezza.

11) «rischio per la sicurezza», la combinazione del livello di pericolo, del livello di vulnerabilità e del potenziale impatto di un evento;

12) «sicurezza nella Commissione», la sicurezza delle persone, delle risorse e delle informazioni nella Commissione, in particolare l'incolumità delle persone e l'integrità delle risorse, l'integrità, la riservatezza e la disponibilità delle informazioni e dei sistemi di comunicazione e informazione, nonché il funzionamento senza ostacoli delle attività operative della Commissione;

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Decisione (94) 2129 della Commissione, dell'8 settembre 1994, relativa ai compiti del servizio di sicurezza.

([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).

13) «misura di sicurezza», ogni misura di sicurezza adottata conformemente alla presente decisione per tenere sotto controllo i rischi per la sicurezza;

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 per la sicurezza», un evento o agente che presumibilmente, in mancanza di una reazione che lo ponga sotto controllo, compromette la sicurezza;

16) «minaccia immediata per la sicurezza» una minaccia per la sicurezza che si verifica senza preavviso o con preavviso estremamente breve;

17) «grave minaccia per la sicurezza», una minaccia per la sicurezza che presumibilmente può comportare perdite di vite umane, gravi lesioni o danni personali, ingenti danni materiali, compromissione di informazioni altamente sensibili, perturbazione dei sistemi informatici o delle capacità operative essenziali della Commissione;

18) «vulnerabilità», una debolezza di qualsiasi tipo che presumibilmente, se fruttata per una o più minacce, compromette la sicurezza nella Commissione.

Articolo 2

Oggetto

1. La presente decisione stabilisce gli obiettivi, i principi fondamentali, l'organizzazione e le responsabilità in relazione alla sicurezza presso la Commissione.

2. La presente decisione si applica a tutti i servizi e in tutti i locali della Commissione. Il personale della Commissione che lavora nelle delegazioni dell'Unione è soggetto alle norme di sicurezza del Servizio europeo per l'azione esterna ([2]).

3. Fatte salve indicazioni specifiche relative a particolari categorie del personale, la presente decisione si applica ai membri della Commissione, al personale della Commissione che rientra nel campo di applicazione dello 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 ai singoli che hanno accesso a fabbricati o altre risorse della Commissione, o alle informazioni trattate dalla Commissione.

4. Le disposizioni della presente decisione lasciano impregiudicate la decisione 2002/47/CE, ECSC, Euratom della Commissione ([3]), la decisione 2004/563/EC, Euratom della Commissione ([4]), la decisione C(2006) 1623 della Commissione ([5]) e la decisione C(2006) 3602 della Commissione ([6]).

CAPO 2

PRINCIPI

Articolo 3

Principi di sicurezza nella Commissione

1. La Commissione applica la presente decisione nel rispetto dei trattati, in particolare della Carta dei diritti fondamentali e del protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea, degli accordi di cui al considerando 2, delle disposizioni normative nazionali applicabili e dei termini della presente decisione. Se necessario, sarà redatta una comunicazione di sicurezza ai sensi dell'articolo 21, paragrafo 2 per fornire orientamenti in merito.

2. La sicurezza nella Commissione si basa sui principi di legalità, trasparenza, proporzionalità e responsabilità.

3. Per principio di legalità s'intende la stretta adesione al quadro giuridico nell'applicare la presente decisione e la rigorosa ottemperanza alle prescrizioni legali.

([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).

([2]) Decisione 2013/C 190/01 dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 19 aprile 2013, relativa alle norme di sicurezza del Servizio europeo per l'azione esterna (GU C 190 del 29.6.2013, pag. 1).

([3]) 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) che allega le disposizioni relative alla gestione dei documenti.

([4]) Decisione 2004/563/CE, CECA, Euratom della Commissione, del 7 luglio 2004, recante modificazione del suo regolamento interno (GU L 251 del 27.7.2004, pag. 9), che allega le disposizioni relative ai documenti elettronici e digitalizzati.

([5]) C(2006) 1623, del 21 aprile 2006, che istituisce una politica armonizzata in materia sanitaria e di sicurezza sul lavoro per il personale della Commissione europea.

([6]) C(2006) 3602, del 16 agosto 2006, relativa alla sicurezza dei sistemi d'informazione utilizzati dalla Commissione europea.

4. Le misure di sicurezza sono adottate apertamente, salvo se tale approccio rischi di comprometterne gli effetti. I destinatari di una misura di sicurezza sono informati preliminarmente delle ragioni e dell'impatto della misura, salvo se ciò rischi di compromettere l'effetto della misura. In tal caso, il destinatario è informato quando il rischio di compromettere l'effetto della misura di sicurezza è cessato.

5. I servizi della Commissione assicurano che si tenga conto degli aspetti relativi alla sicurezza sin dall'inizio dell'elaborazione e attuazione di politiche, decisioni, programmi, progetti e attività della Commissione di cui i suddetti servizi sono responsabili. A tal fine, essi coinvolgono la direzione generale Risorse umane e sicurezza in generale e il responsabile capo della sicurezza dell'informazione della Commissione sin dalle prime fasi della preparazione.

6. Se opportuno, la Commissione chiede la cooperazione delle autorità competenti dello Stato ospitante, di altri Stati membri e delle istituzioni, agenzie o organi dell'UE, se possibile, tenendo conto delle misure adottate o pianificate da tali autorità per far fronte al rischio per la sicurezza in questione.

Articolo 4

Obbligo di osservanza

1. L'osservanza della presente decisione, delle relative norme di attuazione e delle misure e istruzioni di sicurezza impartite dal personale incaricato è obbligatoria.

2. L'inosservanza delle disposizioni di sicurezza è passiva di azione disciplinare conformemente ai trattati e allo statuto dei funzionari, di sanzioni contrattuali e/o di azione legale nell'ambito delle disposizioni normative e regolamentari nazionali.

CAPO 3

GARANTIRE LA SICUREZZA

Articolo 5

Personale incaricato

1. Solo al personale autorizzato con incarico nominativo conferito dal direttore generale delle risorse umane e della sicurezza, in base alle rispettive funzioni, può essere attribuito il potere di adottare una o più delle seguenti misure:

1) portare armi individuali;

2) condurre le indagini di sicurezza di cui all'articolo 13;

3) adottare le misure di cui all'articolo 12 secondo quanto specificato nell'incarico.

2. Gli incarichi di cui al paragrafo 1 sono conferiti per una durata che non supera il periodo durante il quale la persona interessata detiene il posto o la funzione per cui l'incarico è conferito. Tali incarichi sono conferiti conformemente alle disposizioni applicabili di cui all'articolo 3, paragrafo 1.

3. Per quanto riguarda il personale incaricato, la presente decisione costituisce un'istruzione di servizio ai sensi dell'articolo 21 dello statuto dei funzionari.

Articolo 6

Disposizioni generali relative alle misure di sicurezza

1. Nell'adottare le misure di sicurezza la Commissione, per quanto ragionevolmente possibile, garantisce quanto segue:

a) chiede sostegno o assistenza solo presso il paese interessato, purché tale paese sia uno Stato membro dell'Unione europea o, in caso contrario, uno Stato parte della convenzione europea dei diritti dell'uomo, o garantisca diritti almeno equivalenti a quelli della suddetta convenzione;

b) trasferisce informazioni su una persona a destinatari diversi dalle istituzioni e organismi comunitari, non soggetti alla normativa nazionale adottata in attuazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio ([1]), solo conformemente all'articolo 9 del regolamento (CE) n. 45/2001;

([1]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

c) nei confronti della persona che costituisce una minaccia per la sicurezza sono adottate misure di sicurezza di cui la persona può essere tenuta a sostenere i costi. Tali misure di sicurezza possono essere dirette contro altre persone solo se occorre controllare una minaccia immediata o grave per la sicurezza e se sono soddisfatte le seguenti condizioni:

   a) le misure previste contro la persona che costituisce una minaccia per la sicurezza non possono essere adottate o presumibilmente non avranno efficacia;

   b) la Commissione non può controllare la minaccia per la sicurezza con azioni proprie o non può farlo in modo tempestivo;

   c) la misura non costituisce un pericolo sproporzionato per l'altra persona o per i suoi diritti.

2. La direzione Sicurezza della direzione generale Risorse umane e sicurezza stabilisce un quadro d'insieme delle misure di sicurezza che, in base alle disposizioni legislative e regolamentari dello Stato membro che ospita i locali della Commissione, possono richiedere un'ordinanza del tribunale.

3. La direzione Sicurezza della direzione generale Risorse umane e sicurezza può rivolgersi a un appaltatore per lo svolgimento dei compiti relativi alla sicurezza, sotto la direzione e supervisione della direzione Sicurezza.

Articolo 7

Misure di sicurezza relative alle persone

1. Nei locali della Commissione è accordato alle persone un livello di protezione adeguato tenendo conto degli obblighi di sicurezza.

2. In caso di gravi rischi per la sicurezza, la direzione generale Risorse umane e sicurezza offre una protezione ravvicinata ai membri della Commissione o ad altro personale laddove una valutazione del rischio ne abbia indicato la necessità per garantirne sicurezza e incolumità.

3. In caso di gravi rischi per la sicurezza, la Commissione può ordinare l'evacuazione dei locali.

4. Le vittime di incidenti o attentati nei locali della Commissione ricevono assistenza.

5. Per prevenire e controllare i rischi per la sicurezza, il personale incaricato può procedere a controlli dei precedenti delle persone che rientrano nell'ambito di applicazione della presente decisione, al fine di stabilire se il loro accesso ai locali o alle informazioni della Commissione presenti una minaccia per la sicurezza. A tal fine, e conformemente al regolamento (CE) n. 45/2001 e alle disposizioni di cui all'articolo 3, paragrafo 1, il personale incaricato può:

a) avvalersi di tutte le fonti d'informazione disponibili alla Commissione, tenendo conto dell'affidabilità della fonte;

b) accedere al fascicolo personale o ai dati che la Commissione detiene sulle persone che assume o intende assumere, o a quelli del personale dell'appaltatore, se debitamente giustificato.

Articolo 8

Misure di sicurezza concernenti la sicurezza fisica e le risorse

1. La sicurezza delle risorse è garantita dall'applicazione di opportune misure di protezione fisica e tecnica e delle procedure corrispondenti, di seguito «misure di sicurezza fisica» che costituiscono un sistema multistrato.

2. A norma del presente articolo si possono adottare misure intese alla protezione delle persone e delle informazioni nella Commissione, nonché delle risorse.

3. La sicurezza fisica ha i seguenti obiettivi:

— prevenire atti di violenza diretti a membri della Commissione o a persone che rientrano nel campo d'applicazione della presente decisione;

— prevenire lo spionaggio e l'ascolto indiscreto di informazioni sensibili o classificate;

— prevenire il furto, gli atti di vandalismo, sabotaggio o altre azioni violente intese a danneggiare o distruggere edifici e risorse della Commissione;

— rendere possibile l'indagine sugli incidenti in materia di sicurezza anche tramite controlli dei registri di entrata e di uscita, videosorveglianza, registrazioni telefoniche e dati analoghi di cui all'articolo 22, paragrafo 2 di seguito e altre fonti d'informazione.

4. La sicurezza fisica comprende:

— una politica d'accesso applicabile alle persone e ai veicoli che devono accedere ai locali della Commissione, comprese le aree di parcheggio;

— un sistema di controllo dell'accesso che comprende guardie, attrezzature e misure tecniche, sistemi d'informazione o una combinazione dei suddetti elementi.

5. Per garantire la sicurezza fisica, si può procedere come segue:

— registrare l'entrata e l'uscita dai locali della Commissione di persone, veicoli, beni e attrezzature;

— controllare l'identità nei locali;

— ispezionare veicoli, beni e attrezzature con mezzi visivi o tecnici;

— impedire a persone, veicoli e beni non autorizzati di accedere ai locali della Commissione.

Articolo 9

Misure di sicurezza relative alle informazioni

1. La sicurezza dell'informazione copre tutte le informazioni trattate dalla Commissione.

2. A prescindere dalla forma, la sicurezza dell'informazione deve poter conciliare trasparenza, proporzionalità, responsabilità ed efficienza con l'esigenza di proteggere l'informazione contro l'accesso, l'uso, la diffusione, la modifica o la distruzione senza autorizzazione.

3. Obiettivo della sicurezza dell'informazione è la protezione della riservatezza, dell'integrità e della disponibilità.

4. Per classificare le informazioni e per elaborare misure, procedure e norme di sicurezza proporzionate, misure di mitigazione comprese, si ricorre alle procedure di gestione del rischio.

5. I suddetti principi generali alla base della sicurezza dell'informazione si applicano in particolare per quanto riguarda:

a) le «informazioni classificate UE» (di seguito «ICUE»), ossia 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;

b) le «informazioni sensibili non classificate», ossia le informazioni o il materiale che la Commissione deve tutelare in forza degli obblighi giuridici iscritti nei trattati o nei relativi atti di esecuzione, e/o in ragione della loro sensibilità. Le informazioni sensibili non classificate comprendono, ma non solo, le informazioni e il materiale coperti dal segreto professionale di cui all'articolo 339 del TFUE, le informazioni concernenti gli interessi tutelati nell'articolo 4 del regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio [1] in combinato disposto con la giurisprudenza della Corte di giustizia dell'Unione europea, e i dati personali che rientrano nell'ambito di applicazione del regolamento (CE) n. 45/2001.

6. Il trattamento e la conservazione delle informazioni sensibili non classificate sono regolamentati. Tali informazioni sono comunicate solo alle persone che hanno una «necessità di conoscere». Se ritenuto necessario per proteggerne la riservatezza, sono identificate da un contrassegno di sicurezza con istruzioni di trattamento corrispondenti approvate dal direttore generale delle risorse umane e della sicurezza. Se trattate o conservate nei sistemi di comunicazione e informazione, tali informazioni sono protette anche conformemente alla decisione (2006) 3602 e relative norme di attuazione e standard corrispondenti.

7. La persona responsabile della compromissione o della perdita di ICUE o di informazioni sensibili non classificate, riconosciute tali nelle disposizioni che ne disciplinano il trattamento e la conservazione, è passibile di azione disciplinare conformemente allo statuto dei funzionari. L'azione disciplinare non pregiudica eventuali azioni legali o penali delle autorità nazionali competenti degli Stati membri secondo le rispettive disposizioni legislative e regolamentari, né i rimedi contrattuali.

[1] 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).

Articolo 10

Misure di sicurezza relative ai sistemi di comunicazione e informazione

1. Tutti i sistemi di comunicazione e informazione («CIS») in uso alla Commissione si conformano alla politica della Commissione in materia di sicurezza dei sistemi d'informazione stabilita dalla decisione (2006) 3602 e relative norme di attuazione e standard corrispondenti.

2. I servizi della Commissione che detengono, gestiscono o elaborano CIS permettono solo ad altre istituzioni, agenzie, organi o organizzazioni dell'UE di avere accesso a tali sistemi purché dette istituzioni, agenzie, organi o organizzazioni dell'Unione offrano ragionevoli garanzie di protezione dei rispettivi sistemi IT, a livello equivalente a quello della politica della Commissione in materia di sicurezza dei sistemi d'informazione stabilita dalla decisione (2006) 3602 e relative norme di attuazione e standard corrispondenti. La Commissione controlla tale conformità e, in caso di grave o ripetuta inosservanza, ha facoltà di negare l'accesso.

Articolo 11

Analisi forense relativa alla sicurezza informatica

La direzione generale Risorse umane e sicurezza è in particolare responsabile dello svolgimento dell'analisi tecnica forense in collaborazione con i servizi della Commissione competenti a sostegno delle indagini di sicurezza di cui all'articolo 13, in relazione a controspionaggio, perdita di dati, attacchi informatici, sicurezza dei sistemi d'informazione.

Articolo 12

Misure di sicurezza relative alle persone e alle cose

1. Per garantire la sicurezza nella Commissione e al fine di evitare e tenere sotto controllo i rischi, il personale incaricato a norma dell'articolo 5 può, secondo i principi definiti nell'articolo 3, prendere tra l'altro una o più delle misure seguenti:

a) la messa in sicurezza dei luoghi e delle prove, compresi i registri di controllo delle entrate e delle uscite e le immagini di videosorveglianza in caso d'incidenti o di comportamenti che possono comportare procedimenti amministrativi, disciplinari, civili o penali;

b) misure limitate nei confronti di persone che costituiscono una minaccia per la sicurezza, tra le quali l'ordine di uscire dai locali della Commissione, l'accompagnamento di persone fuori dai locali della Commissione, il divieto di accesso ai locali della Commissione per un periodo di tempo fissato in base a criteri da definire nelle norme di attuazione;

c) misure limitate nei confronti degli oggetti che costituiscono una minaccia per la sicurezza, tra le quali la rimozione, il sequestro e l'eliminazione;

d) la perquisizione dei locali della Commissione, uffici compresi;

e) la perquisizione dei CIS e delle attrezzature, dei dati del traffico telefonico e delle telecomunicazioni, dei registri, dei conti utenti ecc;

f) altre misure di sicurezza specifiche con effetto analogo per evitare o tenere sotto controllo i rischi per la sicurezza, in particolare nel contesto dei diritti della Commissione in quanto proprietario o datore di lavoro secondo le disposizioni legislative nazionali applicabili.

2. In circostanze eccezionali, i membri del personale della direzione Sicurezza della direzione generale Risorse umane e sicurezza, incaricati a norma dell'articolo 5, possono prendere le misure d'emergenza necessarie nel rigoroso rispetto dei principi definiti nell'articolo 3. Non appena possibile dopo aver preso le suddette misure, essi informano il direttore della direzione Sicurezza, che richiede presso il direttore generale delle risorse umane e della sicurezza il mandato di conferma delle misure prese e di autorizzazione di eventuali ulteriori azioni necessarie, e si mette in contatto, se opportuno, con le autorità nazionali competenti.

3. Le misure di sicurezza di cui al presente articolo sono documentate nel momento in cui sono prese o, in presenza di rischio immediato o in una situazione di crisi, in un tempo successivo ragionevole. In quest'ultimo caso la documentazione deve includere anche gli elementi su cui si basa la valutazione della presenza di un rischio immediato o di una situazione di crisi. La documentazione può essere concisa, ma deve essere costituita in modo da permettere alla persona oggetto della misura di esercitare i propri diritti di difesa e di protezione dei dati personali conformemente al regolamento (CE) n. 45/2001, e da consentire un esame della legittimità della misura. Nessuna informazione su misure di sicurezza specifiche dirette a un membro del personale è riportata nel fascicolo personale.

4. Nel prendere le misure di sicurezza di cui al punto b), la Commissione garantisce inoltre che la persona in questione abbia la possibilità di contattare un avvocato o una persona di fiducia e che sia informata del diritto di ricorrere al garante europeo della protezione dei dati.

Articolo 13

Indagini

1. Fatti salvi l'articolo 86 e l'allegato IX dello statuto, ed eventuali regimi speciali tra la Commissione e il SEAE, come quello firmato il 28 maggio 2014 tra la direzione generale Risorse umane e sicurezza della Commissione europea e il Servizio europeo per l'azione esterna relativo all'obbligo di diligenza nei confronti del personale della Commissione assegnato alle delegazioni dell'Unione, le indagini di sicurezza si possono svolgere:

a) in caso di incidenti concernenti la sicurezza nella Commissione, anche per sospetti reati penali;

b) in caso di potenziale perdita, manomissione o compromissione di informazioni sensibili non classificate, ICUE o informazioni Euratom classificate;

c) in un contesto di controspionaggio o antiterrorismo;

d) in caso di gravi incidenti informatici.

2. La decisione di svolgere un'indagine di sicurezza è presa dal direttore generale delle risorse umane e della sicurezza, che è anche il destinatario del rapporto d'indagine.

3. Le indagini di sicurezza sono svolte solo da membri abilitati del personale della direzione generale Risorse umane e sicurezza, debitamente incaricate in conformità all'articolo 5.

4. Il personale incaricato esercita i propri poteri in materia di sicurezza in modo indipendente, come specificato nell'incarico, e dispone dei poteri di cui all'articolo 12.

5. Il personale incaricato e competente nello svolgimento delle indagini di sicurezza può raccogliere informazioni da tutte le fonti disponibili in relazione a reati amministrativi o penali commessi nei locali della Commissione o che implichino le persone di cui all'articolo 2, paragrafo 3, siano esse vittime o autori di tali reati.

6. La direzione generale Risorse umane e sicurezza informa le autorità competenti dello Stato membro ospitante o di altri Stati membri interessati, se opportuno, in particolare laddove l'esito dell'indagine presenti indicazioni di un reato penale. In tale contesto, la direzione generale Risorse umane e sicurezza, se opportuno o necessario, può fornire assistenza alle autorità competenti dello Stato membro ospitante o di altri Stati membri interessati.

7. In caso di gravi incidenti informatici, la direzione generale dell'Informatica collabora strettamente con la direzione generale Risorse umane e sicurezza per offrire assistenza in tutte le questioni tecniche. La direzione generale Risorse umane e sicurezza decide, in consultazione con la direzione generale dell'Informatica, dell'opportunità di informare le autorità competenti dello Stato ospitante o di altri Stati membri interessati. Per quanto riguarda il sostegno ad altre istituzioni e agenzie dell'UE potenzialmente interessate, si ricorre ai servizi di coordinamento degli incidenti della squadra di pronto intervento informatico delle istituzioni, organi e agenzie europei (Computer Emergency Response Team, CERT-UE).

8. Le indagini di sicurezza sono documentate.

Articolo 14

Definizione delle competenze nelle indagini di sicurezza e di altro tipo

1. La direzione Sicurezza della direzione generale Risorse umane e sicurezza, se svolge indagini di sicurezza di cui all'articolo 13 e se dette indagini rientrano nelle competenze dell'Ufficio europeo per la lotta antifrode (OLAF) o dell'ufficio di indagine e disciplina della Commissione (IDOC), si mette immediatamente in contatto con tali organi al fine, in particolare, di non compromettere le fasi successive dell'OLAF o dell'IDOC. Se opportuno, la direzione Sicurezza della direzione generale Risorse umane e sicurezza invita l'OLAF e l'IDOC a partecipare all'indagine.

2. Le indagini di sicurezza di cui all'articolo 13 non pregiudicano i poteri dell'OLAF e dell'IDOC definiti nelle disposizioni che disciplinano tali organi. Alla direzione Sicurezza della direzione generale Risorse umane e sicurezza può esser chiesto di fornire assistenza tecnica a indagini avviate dall'OLAF o dall'IDOC.

3. Alla direzione Sicurezza della direzione generale Risorse umane e sicurezza può esser chiesto di assistere agenti dell'OLAF che accedono ai locali della Commissione in conformità all'articolo 3, paragrafo 5 e all'articolo 4, paragrafo 4 del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio ([1]), per agevolarne i compiti. La

([1]) Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

direzione Sicurezza informa di tali richieste di assistenza il segretario generale e il direttore generale della direzione generale Risorse umane e sicurezza o, se l'indagine si svolge nei locali della Commissione occupati dai suoi membri o dal segretario generale, il presidente della Commissione e il commissario responsabile delle risorse umane.

4. Fatto salvo l'articolo 22, lettera a), dello statuto, se un caso rientra nella competenza sia della direzione Sicurezza della direzione generale Risorse umane e sicurezza sia dell'IDOC, la direzione Sicurezza, nel riferire al direttore generale delle risorse umane e della sicurezza conformemente all'articolo 13, valuta nella fase più precoce possibile se vi siano motivi che giustifichino l'affidamento della questione a IDOC. Questa fase si considera raggiunta in particolare quando la situazione di minaccia immediata è cessata. Il direttore generale delle risorse umane e della sicurezza decide in merito.

5. Se un caso rientra nella competenza sia della direzione sicurezza della direzione generale Risorse umane e sicurezza sia dell'OLAF, la direzione Sicurezza riferisce al direttore generale delle Risorse umane e della sicurezza e ne informa il direttore generale dell'OLAF nella fase più precoce possibile. Questa fase si considera raggiunta in particolare quando la situazione di minaccia immediata è cessata. Il direttore generale delle risorse umane e della sicurezza decide in merito.

Articolo 15

Ispezioni di sicurezza

1. La direzione generale Risorse umane e sicurezza avvia ispezioni di sicurezza per verificare che i servizi della Commissione e le persone interessate si conformino alla presente decisione e alle relative norme di attuazione e, se necessario, formulare raccomandazioni.

2. Laddove opportuno, la direzione generale Risorse umane e sicurezza avvia ispezioni di sicurezza o controlli di sicurezza o visite di valutazione, per verificare se il personale, le risorse e le informazioni della Commissione posti sotto la responsabilità di altre istituzioni, agenzie o organi dell'Unione, o degli Stati membri, di Stati terzi o di organizzazioni internazionali, siano adeguatamente protetti secondo disposizioni normative e regolamentari almeno equivalenti a quelle della Commissione. Se opportuno e in uno spirito di collaborazione tra amministrazioni, le suddette ispezioni di sicurezza comprendono anche quelle svolte nel contesto dello scambio di informazioni classificate con altre istituzioni, agenzie o organi dell'Unione, o degli Stati membri, di Stati terzi o di organizzazioni internazionali.

3. Il presente articolo è applicato, mutatis mutandis, al personale della Commissione assegnato alle delegazioni dell'Unione, fatti salvi eventuali regimi speciali tra la Commissione e il SEAE, come quello firmato il 28 maggio 2014 tra la direzione generale Risorse umane e sicurezza della Commissione europea e il Servizio europeo per l'azione esterna relativo all'obbligo di diligenza nei confronti del personale della Commissione assegnato alle delegazioni dell'Unione.

Articolo 16

Stati di allerta e gestione delle situazioni di crisi

1. La direzione generale Risorse umane e sicurezza è responsabile della disposizione di opportune misure relative allo stato di allerta, preliminarmente o in risposta a minacce e incidenti che interessano la sicurezza della Commissione, e delle misure necessarie alla gestione delle situazioni di crisi.

2. Le misure relative allo stato di allerta di cui al paragrafo 1 sono commisurate al livello di minaccia per la sicurezza. I livelli dello stato di allerta sono definiti in stretta collaborazione con i servizi competenti di altre istituzioni, agenzie o organi dell'Unione, o dello Stato membro o degli Stati membri che ospitano i locali della Commissione.

3. La direzione generale Risorse umane e sicurezza è il punto di contatto per gli stati di allerta e di gestione delle situazioni di crisi.

CAPO 4

ORGANIZZAZIONE

Articolo 17

Competenze generali dei servizi della Commissione

1. Le responsabilità della Commissione di cui alla presente decisione sono esercitate dalla direzione generale Risorse umane e sicurezza sotto l'autorità e responsabilità del membro della Commissione responsabile della sicurezza.

2. Le modalità specifiche riguardanti la sicurezza informatica sono definite nella decisione (2006) 3602.

3. Le responsabilità di attuazione della presente decisione con le relative norme di attuazione, e dell'osservanza quotidiana possono essere delegate ad altri servizi della Commissione, laddove il decentramento della sicurezza offra garanzie di efficienza, risparmio di tempo o di risorse, ad esempio grazie all'ubicazione geografica dei servizi interessati.

4. Quando si applica il paragrafo 3, la direzione generale Risorse umane e sicurezza e se opportuno il direttore generale dell'informatica, concludono accordi con i singoli servizi della Commissione volti a definire chiaramente ruoli e responsabilità per l'attuazione e il controllo delle politiche di sicurezza.

Articolo 18

Direzione generale Risorse umane e Sicurezza

1. La direzione generale Risorse umane e sicurezza è in particolare responsabile di quanto segue:

1) elaborare la politica di sicurezza della Commissione, le norme di attuazione e le comunicazioni di sicurezza;

2) raccogliere informazioni al fine di valutare le minacce e i rischi per la sicurezza su tutte le questioni che potrebbero compromettere la sicurezza nella Commissione;

3) fornire controsorveglianza elettronica e protezione a tutti i siti della Commissione, tenendo debitamente conto delle valutazioni della minaccia e delle prove di attività non autorizzate contro gli interessi della Commissione;

4) offrire ai servizi e al personale della Commissione prestazioni di emergenza 24 ore su 24, 7 giorni su 7 sulle questioni connesse alla sicurezza;

5) attuare le misure di sicurezza volte a mitigare i rischi per la sicurezza e a sviluppare e provvedere alla manutenzione dei CIS a copertura di tutte le esigenze operative, in particolare nel settore del controllo dell'accesso fisico, dell'amministrazione delle autorizzazioni di sicurezza e del trattamento delle informazioni sensibili e classificate UE;

6) sensibilizzare, organizzare esercizi ed esercitazioni, formazione e consulenza su tutte le questioni relative alla sicurezza nella Commissione, al fine di promuovere una cultura della sicurezza e creare una squadra di membri del personale adeguatamente formata nelle questioni relative alla sicurezza.

2. La direzione generale Risorse umane e sicurezza, fatte salve le competenze e responsabilità degli altri servizi della Commissione, assicura un collegamento esterno:

1) con i servizi di sicurezza delle altre istituzioni, agenzie o organi dell'Unione sulle questioni relative alla sicurezza delle persone, delle risorse e delle informazioni nella Commissione;

2) con i servizi di sicurezza, di intelligence e di valutazione della minaccia, comprese le autorità nazionali competenti in materia, degli Stati membri, dei paesi terzi e di organizzazioni e organi internazionali su questioni relative alla sicurezza delle persone, delle risorse e delle informazioni nella Commissione;

3) con la polizia e altri servizi di emergenza su tutte le questioni relative alla sicurezza della Commissione in situazioni sia normali che di emergenza;

4) con le autorità di sicurezza delle altre istituzioni, agenzie od organi dell'Unione, degli Stati membri e dei paesi terzi nel settore della reazione agli attacchi informatici con potenziale impatto sulla sicurezza nella Commissione;

5) per quanto riguarda il ricevimento, la valutazione e l'inoltro di intelligence relativa a minacce dovute ad attività terroristiche o di spionaggio che hanno un impatto sulla sicurezza nella Commissione;

6) per quanto riguarda le questioni relative alle informazioni classificate come ulteriormente precisato nella decisione (EU, Euratom) 2015/444 della Commissione ([1]).

3. La direzione generale Risorse umane e sicurezza è responsabile della trasmissione sicura delle informazioni effettuata ai sensi del presente articolo, compresa la trasmissione di dati personali.

Articolo 19

Gruppo di esperti di sicurezza della Commissione (ComSEG)

È istituito un gruppo di esperti di sicurezza della Commissione, incaricato di assistere la Commissione, se opportuno, sulle questioni relative alla politica di sicurezza interna e più specificamente sulla protezione delle informazioni classificate UE.

([1]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per la protezione delle informazioni classificate UE (cfr. pagina 53 della presente Gazzetta ufficiale).

Articolo 20

Responsabili locali della sicurezza (LSOs)

1. Ciascun servizio e gabinetto della Commissione nomina un responsabile locale della sicurezza (LSO), che agisce come principale punto di contatto tra il proprio servizio e la direzione generale Risorse umane e sicurezza per tutte le questioni inerenti alla sicurezza nella Commissione. Se opportuno, è possibile nominare uno o più LSO. L'LSO è un funzionario o un agente temporaneo.

2. In quanto principale punto di contatto sulla sicurezza all'interno del proprio servizio o gabinetto della Commissione, l'LSO, riferisce a intervalli regolari alla direzione generale Risorse umane e sicurezza e alla propria gerarchia in merito alle questioni di sicurezza che riguardano il proprio servizio e, immediatamente in merito agli incidenti della sicurezza, compresi quelli in cui possono essere state compromesse ICUE o informazioni sensibili non classificate.

3. Per le questioni relative alla sicurezza dei sistemi di comunicazione e informazione, l'LSO prende contatto con il responsabile della sicurezza informatica a livello locale (LISO) del proprio servizio della Commissione, il cui ruolo e responsabilità sono definiti nella decisione C(2006) 3602.

4. Egli contribuisce alle attività di formazione e sensibilizzazione in materia di sicurezza che rispondono alle esigenze specifiche del personale, degli appaltatori e di altre persone che lavorano sotto l'autorità del suddetto servizio della Commissione.

5. Su richiesta della direzione generale Risorse umane e sicurezza possono essere affidati all'LSO compiti specifici in caso di rischi gravi o immediati per la sicurezza o in caso di emergenza. Il direttore generale o il direttore delle risorse umane della direzione generale dell'LSO è informato di tali compiti specifici dalla direzione generale Risorse umane e sicurezza.

6. Le responsabilità dell'LSO non pregiudicano il ruolo e le responsabilità assegnati ai responsabili della sicurezza informatica a livello locale (LISO), ai quadri direzionali della salute e sicurezza, ai funzionari di controllo del registro (RCO) o ad altri funzionari con responsabilità connesse alla sicurezza. L'LSO prende contatto con essi per assicurare un approccio coerente e omogeneo alla sicurezza e un flusso efficiente di informazioni su questioni relative alla sicurezza nella Commissione.

7. L'LSO ha accesso diretto al proprio direttore generale o al capo servizio, e tiene informata la gerarchia diretta. Egli dispone di un'autorizzazione di accesso alle ICUE almeno fino al livello SECRET UE/EU SECRET.

8. Per promuovere lo scambio di informazioni e migliori pratiche, la direzione generale Risorse umane e sicurezza organizza una conferenza LSO almeno due volte all'anno; la partecipazione degli LSO è obbligatoria.

CAPO 5

ATTUAZIONE

Articolo 21

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.

CAPO 6

DISPOSIZIONI VARIE E FINALI

Articolo 22

Trattamento dei dati personali

1. La Commissione tratta i dati personali necessari per attuare la presente decisione conformemente al regolamento (CE) n. 45/2001.

2. Fatte salve le misure già in vigore al momento dell'adozione della presente decisione e notificate al garante europeo della protezione dei dati ([1]), le disposizioni nell'ambito della presente decisione che implichino il trattamento di dati personali, quali i dati relativi ai registri di entrata e di uscita, alla videosorveglianza, alle registrazioni di chiamate telefoniche a uffici o centrali di permanenza o dati affini, necessari per motivi di sicurezza o di reazione a situazioni di crisi, sono oggetto di norme di attuazione conformemente all'articolo 21, che stabilisce adeguate garanzie a tutela delle persone interessate.

3. Il direttore generale della direzione generale Risorse umane e sicurezza è responsabile della sicurezza del trattamento dei dati personali nell'ambito della presente decisione.

4. Le norme e procedure di attuazione sono adottate previa consultazione del responsabile della protezione dei dati e del garante europeo della protezione dei dati conformemente al regolamento (CE) n. 45/2001.

Articolo 23

Trasparenza

La presente decisione e le relative norme di attuazione sono rese note al personale della Commissione e a tutte le persone cui si applicano.

Articolo 24

Abrogazione delle precedenti decisioni

La decisione (94) 2129 è abrogata.

Articolo 25

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]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

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

ISSN 1977-0707 (edizione elettronica)
ISSN 1725-258X (edizione cartacea)

Ufficio delle pubblicazioni dell'Unione europea
2985 Lussemburgo
LUSSEMBURGO

IT