II

(Comunicazioni)

COMUNICAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA

PARLAMENTO EUROPEO

DECISIONE DELL'UFFICIO DI PRESIDENZA DEL PARLAMENTO EUROPEO

del 15 aprile 2013

sulla regolamentazione relativa al trattamento delle informazioni riservate da parte del Parlamento europeo

(2014/C 96/01)

L'UFFICIO DI PRESIDENZA DEL PARLAMENTO EUROPEO,

visto l'articolo 23, paragrafo 12 del regolamento del Parlamento europeo,

considerando quanto segue:

(1) Alla luce del nuovo accordo quadro sulle relazioni tra il Parlamento europeo e la Commissione europea ([1]), firmato il 20 ottobre 2010 («l'accordo quadro») e dell'accordo interistituzionale tra il Parlamento europeo e il Consiglio relativo alla trasmissione al Parlamento europeo e al trattamento da parte di quest'ultimo delle informazioni classificate detenute dal Consiglio su materie che non rientrano nel settore della politica estera e di sicurezza comune ([2]), firmato il 12 marzo 2014 (l'«accordo interistituzionale») è necessario stabilire norme specifiche per il trattamento delle informazioni riservate da parte del Parlamento europeo.

(2) Il trattato di Lisbona attribuisce nuovi compiti al Parlamento europeo e, al fine di sviluppare le attività di quest'ultimo nei settori che richiedono un certo grado di riservatezza, è necessario stabilire principi base, norme minime di sicurezza e procedure adeguate per il trattamento da parte del Parlamento europeo delle informazioni riservate, comprese quelle classificate *(classified)*.

(3) La regolamentazione contenuta nella presente decisione mira a garantire livelli equivalenti di protezione e compatibilità con le norme adottate da altre istituzioni, organi e organismi istituiti in virtù o sulla base dei trattati o dagli Stati membri al fine di agevolare il buon funzionamento del processo decisionale dell'Unione europea.

(4) Le disposizioni della presente decisione lasciano impregiudicate le norme vigenti e future relative all'accesso ai documenti adottate in conformità dell'articolo 15 del trattato sul funzionamento dell'Unione europea (TFUE).

([1]) GU L 304 del 20.11.2010, pag. 47.
([2]) GU C 95 del 1.4.2014, pag. 1.

(5) Le disposizioni della presente decisione lasciano impregiudicate le norme vigenti e future relative alla protezione dei dati di carattere personale adottate in conformità dell'articolo 16 TFUE.

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Obiettivo

La presente decisione disciplina la gestione e il trattamento delle informazioni riservate da parte del Parlamento europeo, comprese la creazione, la ricezione, la trasmissione e la conservazione di tali informazioni ai fini di un'adeguata tutela della loro natura riservata. Essa attua l'accordo interistituzionale e l'accordo quadro, in particolare, l'allegato II di quest'ultimo.

Articolo 2

Definizioni

Ai fini della presente decisione si applicano le seguenti definizioni:

a) «informazione», qualsiasi informazione scritta o orale indipendentemente da quale sia il supporto o l'autore;

b) «informazioni riservate», le «informazioni classificate» e «altre informazioni riservate» non classificate;

c) «informazioni classificate», le «informazioni classificate UE» e «informazioni classificate equivalenti»;

d) «informazioni classificate UE» (ICUE), le informazioni e i materiali, classificati come «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo), «SECRET UE/EU SECRET» (UE segreto), «CONFIDENTIEL UE/EU CONFIDENTIAL» (UE riservatissimo) o «RESTREINT UE/EU RESTRICTED» (UE riservato), la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione o di uno o più Stati membri, indipendentemente dal fatto che le informazioni suddette provengano dall'interno delle istituzioni, organi o organismi istituiti in virtù o sulla base dei trattati. A tal riguardo, le informazioni e i materiali classificati al livello:

— «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo): sono le informazioni e i materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione o di uno o più Stati membri;

— «SECRET UE/EU SECRET» (UE segreto): sono le informazioni e i materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione o di uno o più Stati membri;

— «CONFIDENTIEL UE/EU CONFIDENTIAL» (UE riservatissimo): sono le informazioni e i materiali la cui divulgazione non autorizzata potrebbe nuocere agli interessi fondamentali dell'Unione o di uno o più Stati membri;

— «RESTREINT UE/EU RESTRICTED» (UE riservato): sono le informazioni e i materiali la cui divulgazione non autorizzata potrebbe pregiudicare gli interessi dell'Unione o di uno o più Stati membri;

e) «informazioni classificate equivalenti» indica informazioni classificate provenienti dagli Stati membri, da Stati terzi o da organizzazioni internazionali recanti un contrassegno di classifica di sicurezza equivalente a un contrassegno di classifica di sicurezza impiegato per le ICUE e che sono state trasmesse al Parlamento europeo dal Consiglio o dalla Commissione;

f) «altre informazioni riservate» indica qualsiasi altra informazione riservata non classificata, incluse le informazioni coperte dalle disposizioni sulla protezione dei dati o dal segreto d'ufficio, create in seno al Parlamento europeo o trasmesse a quest'ultimo da altre istituzioni, organismi, agenzie istituite in virtù o sulla base dei trattati o da Stati membri;

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

h) «materiale» indica qualsiasi documento o elemento di macchinario o attrezzatura, sia sotto forma di prodotto finito sia in corso di lavorazione;

i) «necessità di sapere» indica la necessità di una persona di accedere a informazioni riservate in modo da essere in grado di svolgere funzioni o compiti ufficiali;

j) «autorizzazione» indica una decisione adottata dal Presidente, se riguarda deputati al Parlamento europeo, o dal Segretario generale, se riguarda funzionari del Parlamento europeo e altri agenti del Parlamento europeo impiegati presso i gruppi politici, con la quale si concede l'accesso individuale alle informazioni classificate fino a un determinato grado, sulla base dell'esito positivo di un'indagine di sicurezza svolta da un'autorità di sicurezza nazionale a norma del diritto nazionale e delle disposizioni di cui all'allegato I, parte 2;

k) «declassamento» indica una riduzione del grado di classificazione;

l) «declassificazione» indica la soppressione di qualsiasi classifica di sicurezza;

m) «contrassegnazione» indica l'apposizione di un contrassegno ad «altre informazioni riservate», inteso a identificare istruzioni specifiche definite in precedenza riguardo al loro trattamento, o il settore coperto da un determinato documento. Un contrassegno può essere apposto anche alle informazioni classificate per imporre requisiti supplementari riguardo al loro trattamento.

n) «rimozione del contrassegno» indica la rimozione di tutti i contrassegni;

o) «originatore» indica l'autore debitamente autorizzato di ***un'***informazione riservata;

p) «comunicazioni di sicurezza» indica misure di attuazione di cui all'allegato II;

q) «istruzioni di trattamento» indica le istruzioni tecniche ai servizi del Parlamento europeo relative alla gestione delle informazioni riservate.

Articolo 3

Principi fondamentali e norme minime

1. Il trattamento delle informazioni riservate da parte del Parlamento segue i principi fondamentali e le norme minime di cui all'allegato I, parte 1.

2. Il Parlamento europeo istituisce un sistema di gestione della sicurezza delle informazioni (Information Security Management System — ISMS) secondo tali principi fondamentali e norme minime. L'ISMS consiste nelle comunicazioni di sicurezza, nelle istruzioni di trattamento e nelle norme applicabili del regolamento. Esso mira a facilitare il lavoro parlamentare e amministrativo, garantendo nel contempo la protezione delle informazioni riservate trattate dal Parlamento europeo, nel pieno rispetto delle norme stabilite dall'originatore di tali informazioni ed enunciate nelle comunicazioni di sicurezza.

Il trattamento delle informazioni riservate mediante i sistemi informativi e di comunicazione automatizzati (CIS) del Parlamento europeo ha luogo secondo il concetto di garanzia di sicurezza delle informazioni (IA), come previsto nella comunicazione di sicurezza 3

3. I deputati al Parlamento europeo possono consultare le informazioni classificate fino al livello «RESTREINT UE/EU RESTRICTED» compreso, senza nulla osta di sicurezza.

4. Quando le informazioni sono classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente, l'accesso é consentito ai deputati al Parlamento europeo autorizzati dal Presidente a norma del paragrafo 5, o previa firma di una dichiarazione solenne con la quale il firmatario si impegna a non divulgare il contenuto di tali informazioni a terzi e a rispettare l'obbligo di proteggere le informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» e si dichiara consapevole delle conseguenze in caso di inadempienza.

5. Quando le informazioni sono classificate di livello «SECRET UE/EU SECRET» o «TRÈS SECRET/EU TOP SECRET» o equivalente, l'accesso é consentito ai deputati al Parlamento europeo autorizzati dal Presidente:

a) previo rilascio del nulla osta di sicurezza a norma dell'allegato I, parte 2, della presente decisione; ovvero

b) previa notifica all'autorità nazionale competente che i deputati interessati sono debitamente autorizzati, in virtù delle loro funzioni, ai sensi del diritto nazionale.

6. Prima che sia loro accordato l'accesso ad informazioni classificate, i deputati al Parlamento europeo sono informati circa le proprie responsabilità in materia di protezione di tali informazioni conformemente all'allegato I e le riconoscono. Essi sono altresì informati sui mezzi per garantire tale protezione.

7. I funzionari del Parlamento europeo e gli altri agenti del Parlamento impiegati presso i gruppi politici possono consultare le informazioni riservate se è accertata la loro «necessità di sapere», e le informazioni di livello superiore a «RESTREINT UE/EU RESTRICTED» se sono muniti dell'adeguato livello di nulla osta di sicurezza. L'accesso alle informazioni riservate è concesso solo se essi sono stati informati e hanno ricevuto istruzioni scritte in merito alle loro responsabilità in materia di protezione di tali informazioni e ai mezzi per garantire tale protezione e se hanno sottoscritto una dichiarazione in cui attestano di aver ricevuto tali istruzioni e si impegnano a rispettarle conformemente alle norme in vigore.

Articolo 4

Creazione di informazioni riservate e loro trattamento amministrativo da parte del Parlamento europeo

1. Il Presidente del Parlamento europeo, i presidenti delle commissioni parlamentari interessate e il Segretario generale e/o qualsiasi persona che egli abbia debitamente autorizzato in forma scritta possono creare informazioni riservate e/o classificare informazioni secondo quanto stabilito dalle comunicazioni di sicurezza.

2. Nel creare informazioni classificate, l'originatore applica il livello adeguato di classificazione in linea con le norme e le definizioni internazionali di cui all'allegato I della presente decisione dell'Ufficio di presidenza. L'originatore determina inoltre, come regola generale, i destinatari che sono autorizzati a consultare le informazioni in base al livello di classificazione. Tale informazione è trasmessa all'Unità per le informazioni classificate (UIC) quando il documento è depositato presso di essa.

3. Le «altre informazioni riservate» coperte da segreto professionale sono trattate conformemente agli allegati I e II e alle istruzioni di trattamento.

Articolo 5

Ricezione di informazioni riservate da parte del Parlamento europeo

1. Le informazioni riservate ricevute dal Parlamento europeo sono comunicate:

a) informazioni di livello «RESTREINT UE/EU RESTRICTED» o equivalente e «altre informazioni riservate»: alla segreteria dell'organo parlamentare/del titolare di un mandato che ne ha fatto richiesta o direttamente all'UIC,

b) informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» o equivalente: all'UIC.

2. La registrazione, la conservazione e la tracciabilità delle informazioni riservate è assicurata, a seconda del caso, dalla segreteria dell'organo parlamentare/del titolare di un mandato che ha ricevuto l'informazione o dall'UIC.

3. Le modalità concordate, da definire di comune accordo, al fine di preservare la riservatezza delle informazioni nel caso di informazioni riservate comunicate dalla Commissione ai sensi dell'allegato II, punto 3.2 dell'accordo quadro, o nel caso di informazioni classificate trasmesse dal Consiglio a norma dell'articolo 5, paragrafo 4, dell'accordo interistituzionale, sono depositate insieme alle informazioni riservate presso la segreteria dell'organo parlamentare/del titolare di un mandato o presso l'UIC, a seconda del caso.

4. Le norme di cui al paragrafo 3 possono essere applicate anche, mutatis mutandis, per la trasmissione di informazioni riservate da parte di altre istituzioni, organi e organismi istituiti in virtù dei trattati o dagli Stati membri.

5. Al fine di assicurare un livello di protezione commisurato al livello di classificazione «TRÈS SECRET UE/EU TOP SECRET» o equivalente, la Conferenza dei presidenti istituisce una commissione di controllo. La comunicazione al Parlamento europeo di informazioni di livello «TRÈS SECRET UE/EU TOP SECRET» o equivalente è soggetta a ulteriori regole, da concordarsi tra il Parlamento europeo e l'istituzione dell'Unione che trasmette le informazioni.

Articolo 6

Comunicazione di informazioni classificate da parte del Parlamento europeo a terzi

Il Parlamento europeo può, previo consenso scritto dell'originatore o dell'istituzione dell'Unione che ha trasmesso le informazioni classificate al Parlamento europeo, a seconda del caso, trasmettere tale informazione classificata a terzi, a condizione che essi garantiscano che, nel trattare tali informazioni, nei loro servizi e locali siano rispettate disposizioni equivalenti a quelle di cui alla presente decisione.

Articolo 7

Strutture protette

1. Ai fini della gestione delle informazioni riservate, il Parlamento europeo predispone una zona protetta e sale di lettura protette.

2. La zona protetta fornisce il necessario per la registrazione, la consultazione, l'archiviazione, la trasmissione e il trattamento delle informazioni riservate. Essa comprende tra l'altro una sala di lettura e una sala di riunioni per la consultazione delle informazioni riservate ed è gestita dall'UIC.

3. Al di fuori della zona protetta, possono essere create sale di lettura protette volte a consentire la consultazione di informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente, e di «altre informazioni riservate». Tali sale di lettura protette sono gestite dai servizi competenti delle segreterie dell'organo parlamentare/del titolare di un mandato o dall'UIC, a seconda del caso. Esse non contengono fotocopiatrici, telefoni, fax, scanner o altri mezzi tecnici di riproduzione o trasmissione di documenti.

Articolo 8

Registrazione, trattamento e conservazione delle informazioni riservate

1. Le informazioni di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate» possono essere registrate e conservate dai servizi competenti delle segreterie dell'organo parlamentare/del titolare di un mandato o dall'UIC, a seconda di chi ha ricevuto l'informazione.

2. Le seguenti disposizioni disciplinano il trattamento delle informazioni di livello «RESTREINT EU/EU RESTRICTED» o equivalente e delle «altre informazioni riservate»:

a) i documenti sono consegnati di persona al capo della segreteria, che li registra ed emette un avviso di ricevimento;

b) quando non sono effettivamente in uso, tali documenti sono conservati in un luogo chiuso, sotto la responsabilità della segreteria;

c) le informazioni non possono in nessun caso essere salvate su un altro supporto o trasmesse a terzi; tali documenti possono essere riprodotti solo mediante attrezzature adeguatamente accreditate precisate nelle comunicazioni di sicurezza;

d) l'accesso a tali informazioni è limitato alle persone indicate dall'originatore o dall'istituzione dell'Unione che ha trasmesso l'informazione al Parlamento europeo, secondo il disposto dell'articolo 4, paragrafo 2 o dell'articolo 5, paragrafi 3, 4 e 5;

e) la segreteria dell'organo parlamentare/del titolare di un mandato tiene un registro delle persone che hanno consultato le informazioni, unitamente alla data e all'ora di tale consultazione e trasmette all'UIC il registro al momento del deposito dell'informazione presso l'UIC.

3. Le informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» o equivalente sono registrate, trattate e conservate dall'UIC nella zona protetta, a seconda degli specifici livelli di classificazione e secondo quanto definito nelle comunicazioni di sicurezza.

4. In caso di violazione delle norme di cui ai paragrafi da 1 a 3, il funzionario responsabile della segreteria dell'organo parlamentare/del titolare di un mandato o dell'UIC, a seconda del caso, informa il Segretario generale, che ne riferisce al Presidente qualora sia interessato un deputato al Parlamento europeo.

Articolo 9

Accesso alle strutture protette

1. Unicamente le seguenti persone hanno accesso alla zona protetta:

a) persone che, a norma dell'articolo 3, paragrafi da 4 a 7, sono autorizzate a consultare le informazioni ivi detenute e che hanno presentato una richiesta a norma dell'articolo 10, paragrafo 1;

b) persone che, a norma dell'articolo 4, paragrafo 1, sono autorizzate a creare informazioni riservate e che hanno presentato una domanda a norma dell'articolo 10, paragrafo 1;

c) i funzionari del Parlamento europeo in servizio presso l'UIC;

d) i funzionari del Parlamento europeo responsabili della gestione del CIS;

e) i funzionari del Parlamento europeo responsabili della sicurezza e della protezione antincendio, quando necessario;

f) il personale di pulizia, ma solo in presenza e sotto stretta sorveglianza di un funzionario in servizio presso l'UIC.

2. L'UIC può rifiutare l'accesso alla zona protetta a chiunque non sia autorizzato. Qualsiasi contestazione di un tale diniego è sottoposta al Presidente qualora si tratti di richieste di accesso da parte di deputati al Parlamento europeo, e al Segretario generale negli altri casi.

3. Il Segretario generale può autorizzare riunioni di un ridotto numero di persone nella sala riunioni situata all'interno della zona protetta.

4. Hanno accesso alla sala di lettura protetta unicamente le persone seguenti:

a) i deputati al Parlamento europeo, i funzionari del Parlamento europeo e gli altri agenti del Parlamento europeo impiegati presso i gruppi politici, debitamente identificati ai fini della consultazione o creazione di informazioni riservate;

b) i funzionari del Parlamento europeo responsabili della gestione del CIS, i funzionari della segreteria dell'organo parlamentare/del titolare di un mandato che hanno ricevuto l'informazione e i funzionari dell'UIC;

c) ove necessario, i funzionari del Parlamento europeo responsabili della sicurezza e della protezione antincendio.

d) il personale di pulizia, ma solo in presenza e sotto stretta sorveglianza di un funzionario in servizio presso la segreteria dell'organo parlamentare/del titolare di un mandato o presso l'UIC, a seconda dei casi.

5. La segreteria competente dell'organo parlamentare/del titolare di un mandato o l'UIC, a seconda dei casi, può rifiutare l'accesso a una sala di lettura protetta a chiunque non sia autorizzato ad accedervi. Qualsiasi contestazione di un tale diniego è sottoposta al Presidente qualora si tratti di richieste di accesso di deputati al Parlamento europeo, e al Segretario generale negli altri casi.

Articolo 10

Consultazione o creazione di informazioni riservate in strutture protette

1. Ogni persona che intenda consultare o creare informazioni riservate all'interno della zona protetta comunica preventivamente il proprio nominativo all'UIC. L'UIC controlla l'identità di tale persona e verifica se essa è autorizzata, a norma dell'articolo 3, paragrafi da 3 a 7, dell'articolo 4, paragrafo 1 o dell'articolo 5, paragrafi da 3 a 5, a consultare o a creare informazioni riservate.

2. Ogni persona che intenda, a norma dell'articolo 3, paragrafi 3 e 7, consultare informazioni riservate classificate di livello «RESTREINT EU/EU RESTRICTED» o equivalente e «altre informazioni riservate» in una sala di lettura protetta comunica preventivamente il proprio nominativo ai servizi competenti della segreteria dell'organo parlamentare/del titolare di un mandato o all'UIC.

3. Salvo circostanze eccezionali (ad esempio, un elevato numero di richieste di consultazione in un breve lasso di tempo), solo un'unica persona alla volta è autorizzata a consultare le informazioni riservate nella struttura protetta, alla presenza di un funzionario della segreteria dell'organo parlamentare/del titolare di un mandato o dell'UIC.

4. Durante il processo di consultazione non sono autorizzati contatti con l'esterno (compreso mediante l'uso del telefono o di strumenti tecnologici), annotazioni né la riproduzione mediante fotocopia o fotografia delle informazioni riservate consultate.

5. Prima di autorizzare una persona a lasciare la struttura protetta, il funzionario della segreteria dell'organo parlamentare/del titolare di un mandato o dell'UIC si assicura che le informazioni riservate consultate siano ancora presenti, integre e complete.

6. In caso di violazione delle norme di cui sopra, il funzionario della segreteria dell'organo parlamentare/del titolare di un mandato o dell'UIC informa il Segretario generale, che ne riferisce al Presidente qualora sia interessato un deputato al Parlamento europeo.

Articolo 11

Norme minime applicabili alla consultazione di informazioni riservate in una riunione a porte chiuse tenuta fuori da strutture protette

1. Le informazioni di livello «RESTREINT EU/EU RESTRICTED» o equivalente, e le «altre informazioni riservate» possono essere consultate dai membri delle commissioni parlamentari o di altri organi politici e amministrativi del Parlamento europeo durante una riunione a porte chiuse tenuta fuori da strutture protette.

2. Nelle circostanze di cui al paragrafo 1, la segreteria dell'organo parlamentare/del titolare di un mandato responsabile della riunione assicura che siano rispettate le condizioni seguenti:

a) solo le persone designate dal presidente della commissione o dall'organo competente a partecipare alla riunione sono autorizzate a entrare nella sala riunioni;

b) i documenti sono numerati, distribuiti all'inizio della riunione e raccolti al termine della stessa; non si prendono note del loro contenuto e non sono eseguite fotocopie o fotografie;

c) il verbale della riunione non fa alcun riferimento al contenuto della discussione dell'informazione trattata; soltanto l'eventuale decisione pertinente può figurare nel processo verbale;

d) le informazioni riservate trasmesse oralmente a destinatari in seno al Parlamento europeo sono soggette a un livello di protezione equivalente a quello applicato alle informazioni riservate trasmesse per iscritto;

e) nella sala riunioni non sono presenti copie supplementari dei documenti;

f) le copie dei documenti sono distribuite ai partecipanti e agli interpreti, all'inizio della riunione, solo in numero necessario;

g) il livello di classificazione/il contrassegno dei documenti è precisato dal presidente della riunione all'inizio della stessa;

h) i partecipanti non rimuovono i documenti dalla sala riunioni;

i) tutte le copie dei documenti sono raccolte e contate alla fine della riunione dalla segreteria dell'organo parlamentare/del titolare di un mandato;

j) non sono introdotti apparecchiature o strumenti elettronici o di comunicazione nella sala riunioni nella quale le informazioni riservate sono consultate o discusse.

3. Nei casi in cui, conformemente alle eccezioni previste all'allegato II, punto 3.2.2, dell'accordo quadro, e all'articolo 6, paragrafo 5, dell'accordo interistituzionale, informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente sono discusse in una riunione a porte chiuse, la segreteria dell'organo parlamentare/del titolare di un mandato responsabile della riunione assicura, oltre al rispetto delle disposizioni previste al paragrafo 2, che le persone designate a partecipare alla riunione soddisfino i requisiti di cui all'articolo 3, paragrafi 4 e 7.

4. Nel caso previsto al paragrafo 3, l'UIC fornisce alla segreteria dell'organo parlamentare/del titolare di un mandato responsabile della riunione a porte chiuse il numero necessario di copie dei documenti da discutere, che sono restituite all'UIC dopo la riunione.

Articolo 12

Archiviazione dei documenti riservati

1. All'interno della zona protetta è assicurato un sistema protetto di archiviazione. L'UIC è responsabile della gestione degli archivi protetti, conformemente ai normali criteri di archiviazione.

2. Le informazioni classificate depositate in via definitiva presso l'UIC e le informazioni di livello «RESTREINT EU/EU RESTRICTED» o equivalente depositate presso la segreteria dell'organo parlamentare/del titolare di un mandato sono trasferite nella sala di archiviazione protetta ubicata nella zona protetta sei mesi dopo l'ultima consultazione e al massimo un anno dopo il loro deposito. Le «altre informazioni riservate», se non sono state depositate presso l'UIC, sono archiviate dalla segreteria dell'organo parlamentare/del titolare di un mandato interessato, conformemente alle regole generali sulla gestione dei documenti.

3. Le informazioni riservate conservate negli archivi protetti possono essere consultate alle seguenti condizioni:

a) sono autorizzate unicamente le persone identificate per nome, per funzione o per carica tramite il documento di accompagnamento stilato al momento del deposito dell'informazione riservata;

b) la domanda di consultazione è presentata all'UIC, che trasferisce il documento in questione alla sala di lettura protetta; e

c) si applicano le procedure e le condizioni che disciplinano la consultazione delle informazioni riservate di cui all'articolo 10.

Articolo 13

Declassamento, declassificazione e rimozione del contrassegno delle informazioni riservate

1. Le informazioni riservate possono essere declassate, declassificate o private del contrassegno unicamente previo consenso dell'originatore e, se necessario, previa discussione con altre parti interessate.

2. Il declassamento o la declassificazione sono confermati per iscritto. L'originatore è tenuto a informare i destinatari del cambiamento di classificazione, e questi ultimi sono a loro volta tenuti a informarne i destinatari successivi ai quali hanno trasmesso l'originale o una copia del documento. Nella misura del possibile, l'originatore indica sul documento classificato la data, un termine o un evento a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia ancora necessaria.

3. Le informazioni riservate conservate negli archivi protetti sono esaminate a tempo debito, e non oltre il 25° anno successivo alla data della loro creazione, per determinare se debbano o meno essere declassificate, declassate o se debba essere rimosso il contrassegno. L'esame e la pubblicazione di tali informazioni si svolge in conformità con le disposizioni del regolamento (CEE, Euratom) n. 354/83 del Consiglio, del 1° febbraio 1983, che rende accessibili al pubblico gli archivi storici della Comunità economica europea e della Comunità europea dell'energia atomica ([1]). La declassificazione è effettuata dall'originatore dell'informazione classificata o dal servizio responsabile a norma dell'allegato I, parte 1, sezione 10.

4. Dopo la declassificazione, le informazioni precedentemente classificate conservate nell'archivio protetto sono trasferite agli archivi storici del Parlamento europeo a fini di conservazione permanente e ulteriore trattamento secondo le norme applicabili.

5. Dopo la rimozione del contrassegno, le «altre informazioni riservate» sono soggette alle regole del Parlamento europeo sulla gestione dei documenti.

Articolo 14

Violazioni della sicurezza, perdita o compromissione di informazioni riservate

1. Una violazione della riservatezza in generale e della presente decisione in particolare comporta, qualora si tratti di deputati al Parlamento europeo, l'applicazione delle pertinenti disposizioni in materia di sanzioni previste dal regolamento del Parlamento europeo.

2. Una violazione commessa da un membro del personale del Parlamento europeo comporta l'applicazione delle procedure e delle sanzioni previste rispettivamente dallo statuto dei funzionari dell'Unione europea e dal regime applicabile agli altri agenti dell'Unione, stabilito dal regolamento (CEE, Euratom, CECA) n. 259/68 («Statuto dei funzionari»).

([1]) GU L 43 del 15.2.1983, pag. 1.

3. Il Presidente e/o il Segretario generale, a seconda del caso, organizzano tutte le indagini necessarie nel caso di una violazione quale definita nella comunicazione di sicurezza 6.

4. Se le informazioni riservate sono state trasmesse al Parlamento europeo da un'istituzione dell'Unione o da uno Stato membro, il Presidente e/o il Segretario generale, a seconda dei casi, informa l'istituzione dell'Unione o lo Stato membro interessati della perdita o compromissione accertata o presunta delle informazioni classificate, dei risultati delle indagini svolte e delle misure adottate per evitare che i fatti si ripetano.

Articolo 15

Adeguamento della presente decisione e delle relative norme di attuazione e relazione annuale sull'applicazione della presente decisione

1. Il Segretario generale propone i necessari adeguamenti della presente decisione e degli allegati recanti le modalità di attuazione e sottopone le proposte per decisione all'Ufficio di presidenza.

2. Il Segretario generale è responsabile dell'attuazione della presente decisione da parte dei servizi del Parlamento europeo ed emana le istruzioni relative al trattamento delle questioni oggetto del sistema di gestione della sicurezza delle informazioni (ISMS) secondo i principi stabiliti dalla presente decisione.

3. Il Segretario generale presenta una relazione annuale all'Ufficio di presidenza sull'applicazione della presente decisione.

Articolo 16

Disposizioni transitorie e finali

1. Le informazioni non classificate depositate presso l'UIC o in altri archivi del Parlamento europeo che sono considerate riservate e hanno data anteriore al 1º aprile 2014 sono considerate, ai fini della presente decisione, come «altre informazioni riservate». L'originatore può modificarne il livello di riservatezza in qualunque momento.

2. In deroga all'articolo 5, paragrafo 1, lettera a), e all'articolo 8, paragrafo 1, della presente decisione, per un periodo di dodici mesi a decorrere dal 1º aprile 2014, le informazioni fornite dal Consiglio a norma dell'accordo interistituzionale, classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente sono depositate presso l'UIC, che le registra e conserva. Tali informazioni possono essere consultate secondo il disposto dell'articolo 4, paragrafo 2, lettere a) e c), e dell'articolo 5, paragrafo 4, dell'accordo interistituzionale.

3. La decisione dell'Ufficio di presidenza del 6 giugno 2011 sulla regolamentazione relativa al trattamento delle informazioni riservate da parte del Parlamento europeo è abrogata.

Articolo 17

Entrata in vigore

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

ALLEGATO I

Parte 1

PRINCIPI FONDAMENTALI E NORME MINIME DI SICUREZZA PER LA PROTEZIONE DELLE INFORMAZIONI RISERVATE

1. **INTRODUZIONE**

Con le presenti disposizioni si espongono i principi fondamentali e le norme minime di sicurezza per la protezione delle informazioni riservate che devono essere osservate dal Parlamento europeo in tutte le sue sedi di servizio, compresi tutti i destinatari di informazioni classificate e «altre informazioni riservate», perché sia salvaguardata la sicurezza e ogni persona interessata abbia la garanzia che è in vigore un regime comune di protezione. Le disposizioni sono completate dalle comunicazioni di sicurezza di cui all'allegato II e dalle altre disposizioni relative al trattamento delle informazioni riservate da parte delle commissioni parlamentari e di altri organi parlamentari/titolari di un mandato.

2. **PRINCIPI GENERALI**

La politica di sicurezza del Parlamento europeo forma parte integrante della sua politica generale di gestione interna e si basa pertanto sugli stessi principi informatori di quest'ultima. Tra questi principi si annoverano la legalità, la trasparenza, la responsabilità (o dovere di rendere conto delle proprie azioni), la sussidiarietà e la proporzionalità.

La legalità implica la necessità di una stretta adesione al quadro giuridico nell'espletamento delle funzioni legate alla sicurezza e la rigorosa ottemperanza alle prescrizioni legali applicabili. Inoltre, le responsabilità nel campo della sicurezza devono fondarsi su adeguate disposizioni normative. Tra queste, trovano piena applicazione le disposizioni dello statuto del personale, in particolare l'articolo 17 sull'obbligo imposto al personale di astenersi dal rivelare senza autorizzazione informazioni ricevute nell'ambito della propria funzione e il titolo VI sulle misure disciplinari. Infine, le violazioni della sicurezza nell'ambito di responsabilità del Parlamento europeo devono essere affrontate in maniera coerente con il suo regolamento e con la sua politica in materia di misure disciplinari.

La trasparenza implica chiarezza in tutte le norme e disposizioni sulla sicurezza, equilibrio nella ripartizione delle competenze tra i vari servizi e settori (sicurezza materiale rispetto alla protezione delle informazioni, ecc.) e un'azione sistematica e strutturata di sensibilizzazione alla tematica della sicurezza. Inoltre, sono necessari chiari orientamenti scritti per l'attuazione delle misure di sicurezza.

La responsabilità implica una chiara definizione dei compiti in materia di sicurezza, da cui discende altresì la necessità di una regolare verifica del corretto esercizio di tali compiti.

La sussidiarietà significa che la sicurezza dev'essere organizzata al livello gerarchico più basso, il più possibile in connessione con le direzioni generali e con i servizi del Parlamento europeo. La proporzionalità implica che gli interventi nel campo della sicurezza devono essere limitati a quanto è assolutamente necessario e le misure di sicurezza devono essere proporzionate agli interessi da tutelare, come pure alle minacce, reali o potenziali, contro tali interessi, così da poterli difendere nel modo che assicuri il minor danno possibile.

3. **FONDAMENTI DELLA SICUREZZA DELL'INFORMAZIONE**

Un'efficace sicurezza delle informazioni si fonda sui seguenti elementi:

a) appropriati sistemi di comunicazione e informazione (CIS), sotto la responsabilità dell'autorità di sicurezza del Parlamento europeo (quale definita nella comunicazione di sicurezza 1;

b) all'interno del Parlamento europeo, l'autorità di garanzia dell'informazione (quale definita nella comunicazione di sicurezza 1 incaricata di collaborare con l'autorità di sicurezza competente per fornire informazioni e consulenza circa le minacce tecniche ai CIS e i relativi mezzi di protezione contro tali minacce;

c) una stretta collaborazione tra i servizi responsabili del Parlamento europeo e i servizi di sicurezza delle altre istituzioni dell'Unione;

4. **PRINCIPI DI SICUREZZA DELLE INFORMAZIONI**

4.1. ***Obiettivi***

La sicurezza delle informazioni persegue principalmente i seguenti obiettivi:

a) proteggere le informazioni riservate dallo spionaggio, da manomissioni o dalla diffusione non autorizzata;

b) proteggere le informazioni classificate impiegate in sistemi e reti di comunicazione e d'informazione da minacce contro la loro riservatezza, integrità e disponibilità;

c) proteggere i locali del Parlamento europeo in cui si trovano le informazioni classificate dal sabotaggio e dal danneggiamento intenzionale premeditato;

d) in caso di incidente di sicurezza, valutare il danno arrecato, limitare le conseguenze, svolgere indagini sulla sicurezza e adottare le misure correttive necessarie.

4.2. ***Classificazione***

4.2.1. Per quanto riguarda la riservatezza, la selezione delle informazioni e dei materiali da proteggere e la valutazione del grado di protezione necessaria richiedono diligenza ed esperienza. È fondamentale che il grado di protezione corrisponda al grado di sensibilità, in termini di sicurezza, richiesto dalla singola informazione e dal singolo materiale da proteggere. Perché non vi siano ostacoli al flusso delle informazioni, occorre evitare sia la sovra- che la sottoclassificazione.

4.2.2. Il sistema di classificazione è lo strumento per tradurre in pratica i principi stabiliti nella presente sezione. Un sistema di classificazione analogo deve essere adottato nella pianificazione e nell'organizzazione della lotta contro lo spionaggio, il sabotaggio, il terrorismo e altre minacce, al fine di garantire la massima protezione ai principali edifici in cui sono contenute informazioni classificate e ai punti più sensibili all'interno di tali edifici.

4.2.3. La responsabilità della classificazione delle informazioni spetta unicamente all'originatore.

4.2.4. Il grado di classificazione può dipendere unicamente dal contenuto delle informazioni stesse.

4.2.5. Quando più elementi d'informazione sono raggruppati tra loro, la loro classificazione è almeno equivalente al grado di classificazione più elevato attribuito a uno dei suoi singoli elementi. Tuttavia, a una raccolta di informazioni può essere attribuito un grado di classificazione più elevato di quello dei suoi elementi costitutivi.

4.2.6. Le classificazioni sono attribuite soltanto nella misura e per la durata in cui sia necessario.

4.3. ***Finalità delle misure di sicurezza***

Le misure di sicurezza:

a) riguardano tutte le persone che hanno accesso alle informazioni classificate, ai supporti contenenti informazioni classificate e alle «altre informazioni riservate», nonché a tutti i locali che contengono tali informazioni e alle installazioni importanti;

b) sono destinate a individuare le persone che, per la loro situazione (in termini di accesso, relazioni o altro), potrebbero mettere in pericolo la sicurezza di tali informazioni o di importanti installazioni che contengono tali informazioni e a provvedere alla loro esclusione o allontanamento;

c) impediscono alle persone non autorizzate di accedere a tali informazioni o alle installazioni che le contengono;

d) garantiscono che tali informazioni siano diffuse soltanto in base al principio della necessità di sapere, che è fondamentale per tutti gli aspetti della sicurezza;

e) assicurano l'integrità (ossia la prevenzione della corruzione, dell'alterazione o della cancellazione non autorizzate) e la disponibilità (per coloro che hanno bisogno e sono autorizzati ad averne accesso) di tutte le informazioni, siano esse classificate o non, e soprattutto qualora esse siano immagazzinate, elaborate o trasmesse sotto forma elettromagnetica.

5. **NORME COMUNI MINIME**

Il Parlamento europeo garantisce che tutti i destinatari di informazioni classificate, all'interno dell'istituzione e nel suo ambito di competenza, segnatamente tutti i suoi servizi e contraenti, osservino norme minime comuni di sicurezza affinché tali informazioni possano essere trasmesse con la certezza che saranno trattate con la stessa diligenza. Dette norme minime includono criteri per il rilascio del nulla osta di sicurezza ai funzionari del Parlamento europeo e altri agenti del Parlamento impiegati presso i gruppi politici, e procedure per la protezione delle informazioni riservate.

Il Parlamento europeo autorizza l'accesso di terzi a tali informazioni solo quando i terzi garantiscono che, nel trattarle, sono rispettate disposizioni almeno strettamente equivalenti alle suddette norme minime.

Dette norme minime comuni si applicano anche quando, in virtù di un contratto o di un accordo di sovvenzione, il Parlamento europeo affida a soggetti industriali o di altra natura mansioni che comportano informazioni riservate.

6. **SICUREZZA DEI FUNZIONARI E ALTRI AGENTI DEL PARLAMENTO EUROPEO IMPIEGATI PRESSO I GRUPPI POLITICI**

6.1. ***Istruzioni di sicurezza per i funzionari del Parlamento europeo e altri agenti impiegati presso i gruppi politici***

I funzionari del Parlamento europeo e altri agenti del Parlamento impiegati presso i gruppi politici che ricoprono incarichi in cui potrebbero aver accesso a informazioni classificate sono dettagliatamente istruiti al momento di assumere l'incarico e poi a intervalli regolari circa la necessità della sicurezza e le relative procedure. Tali persone sono tenute a confermare per iscritto di aver letto e perfettamente capito le norme di sicurezza in vigore.

6.2. ***Responsabilità dei dirigenti***

I dirigenti hanno il dovere di sapere quali dei loro subordinati lavorino a contatto con informazioni classificate o abbiano accesso a sistemi di comunicazione o d'informazione protetti e di registrare e riferire qualsiasi incidente o caso di palese vulnerabilità che possa avere conseguenze sulla sicurezza.

6.3. ***Status di sicurezza dei funzionari del Parlamento europeo e altri agenti del Parlamento impiegati presso i gruppi politici***

Sono istituite procedure per garantire che, allorché si viene a conoscenza di informazioni negative riguardo a un funzionario del Parlamento europeo o un altro agente del Parlamento impiegato presso i gruppi politici, siano prese misure per verificare se costui svolge un lavoro a contatto con informazioni classificate o ha accesso a sistemi di comunicazione o d'informazione protetti e l'ufficio responsabile del Parlamento europeo ne sia informato. Se l'autorità di sicurezza nazionale competente indica che rappresenta un pericolo per la sicurezza, la persona in questione deve essere allontanata o rimossa da ogni incarico in cui potrebbe mettere a repentaglio la sicurezza.

7. **SICUREZZA MATERIALE**

La sicurezza materiale consiste nell'applicazione di misure di protezione fisica e tecnica volte a evitare che persone non autorizzate abbiano accesso alle informazioni classificate.

7.1. ***Necessità di protezione***

Il grado di sicurezza materiale da applicare per garantire la protezione delle informazioni classificate deve essere proporzionato alla classificazione, al volume e alle minacce che incombono sulle informazioni e sul materiale custodito. Tutti i detentori di informazioni classificate devono seguire pratiche uniformi per quanto riguarda la classificazione di tali informazioni in loro possesso e ottemperare a norme comuni di protezione per quel che riguarda la custodia, la trasmissione e la diffusione di informazioni e di materiale soggetti a protezione.

7.2. ***Verifica***

Prima di lasciare i locali in cui sono conservate informazioni classificate senza sorveglianza, le persone che ne hanno la custodia devono accertarsi che le informazioni siano immagazzinate in modo sicuro e che tutti i dispositivi di sicurezza siano stati attivati (serrature, allarmi, ecc.). Al termine dell'orario di lavoro devono essere effettuati altri controlli indipendenti.

7.3. ***Sicurezza degli edifici***

Gli edifici contenenti informazioni classificate o sistemi di comunicazione e d'informazione protetti devono essere tutelati contro l'accesso non autorizzato.

Il tipo di protezione destinato alle informazioni classificate, per esempio sbarramento di finestre, serrature alle porte, guardie all'entrata, sistemi di controllo dell'accesso automatizzati, controlli di sicurezza e ispezioni, sistemi d'allarme, sistemi di individuazione delle intrusioni e cani da guardia dipende:

a) dalla classificazione, dal volume e dall'ubicazione all'interno dell'edificio delle informazioni e dei materiali da proteggere;

b) dalla qualità dei contenitori di sicurezza per le informazioni e i materiali interessati; nonché

c) dalle caratteristiche dell'edificio e dalla sua ubicazione.

Anche per i sistemi di comunicazione e d'informazione il tipo di protezione prescelto deve dipendere da una stima del valore di quanto è in gioco e del danno potenziale che deriverebbe dal venir meno della sicurezza, dalle caratteristiche e dall'ubicazione dell'edificio nel quale è custodito il sistema e dalla collocazione del sistema all'interno dell'edificio.

7.4. ***Piani d'emergenza***

Sono predisposti in anticipo piani dettagliati per assicurare la protezione delle informazioni classificate in caso di emergenza.

8. **INDICAZIONI DI SICUREZZA, CONTRASSEGNI, APPOSIZIONI E GESTIONE DELLA CLASSIFICAZIONE**

8.1. ***Indicazioni di sicurezza***

Non sono consentite classificazioni diverse da quelle definite all'articolo 2, lettera d), della presente decisione.

Possono essere utilizzate indicazioni di sicurezza convenzionali per porre limiti alla validità di una classificazione (per il declassamento o la declassificazione automatica di informazioni classificate).

Le indicazioni di sicurezza sono utilizzate soltanto unitamente a una classificazione.

Le indicazioni di sicurezza sono ulteriormente disciplinate nella comunicazione di sicurezza 2 e definite nelle istruzioni di trattamento.

8.2. ***Contrassegni***

Un contrassegno è usato per specificare istruzioni specifiche prestabilite sul trattamento delle informazioni confidenziali. I contrassegni possono anche indicare il settore che forma oggetto del documento, una distribuzione particolare sulla base del principio della necessità di sapere, o la scadenza di un embargo (nel caso di informazioni non classificate).

Un contrassegno non è una classificazione e non può essere usato al posto di questa.

I contrassegni sono ulteriormente disciplinati nella comunicazione di sicurezza 2 e definiti nelle istruzioni di trattamento.

8.3. ***Apposizione delle classificazioni e delle indicazioni di sicurezza***

L'apposizione delle classificazioni, delle indicazioni di sicurezza e dei contrassegni avviene in conformità della comunicazione di sicurezza 2, sezione E, e delle istruzioni di trattamento.

8.4. ***Gestione della classificazione***

8.4.1. *Prescrizioni generali*

Le informazioni sono classificate solo se necessario. La classificazione è indicata chiaramente e correttamente ed è mantenuta solo per la durata in cui è necessario proteggere l'informazione.

La responsabilità della classificazione dell'informazione e di eventuali declassamenti o declassificazioni successivi spetta unicamente all'originatore.

Il funzionario del Parlamento europeo classifica un'informazione, oppure la declassa o la declassifica su istruzione o per delega del Segretario generale.

Le modalità dettagliate per il trattamento dei documenti classificati sono elaborate in modo da garantire che essi siano soggetti a una protezione commisurata alle informazioni che contengono.

Il numero di persone autorizzate a creare informazioni classificate «TRÈS SECRET UE/EU TOP SECRET» è limitato al minimo e il loro nominativo è registrato in un elenco compilato dall'UIC.

8.4.2. *Attribuzione delle classificazioni*

La classificazione di un documento è determinata dal livello di sensibilità del suo contenuto, secondo la definizione di cui all'articolo 2, lettera d). È importante che la classificazione sia assegnata correttamente e utilizzata con moderazione.

Il grado di classificazione attribuito a una lettera o nota cui è accluso altro materiale corrisponde almeno a quello dell'elemento accluso con grado più elevato. L'originatore indica chiaramente il livello di classificazione da attribuire alla lettera o nota quando è separata dal materiale accluso.

L'originatore di un documento che deve essere classificato segue le disposizioni che precedono ed evita la sovra — o sottoclassificazione.

È possibile che singole pagine, paragrafi, sezioni, annessi, appendici, allegati di un determinato documento e altro materiale accluso richiedano classificazioni differenti: in tal caso, all'insieme del documento viene attribuita la classificazione dell'elemento con grado più elevato.

9. **ISPEZIONI**

La direzione della sicurezza e della valutazione del rischio del Parlamento europeo compie ispezioni periodiche interne delle misure di sicurezza per la protezione delle informazioni classificate; essa può chiedere l'assistenza delle autorità di sicurezza del Consiglio o della Commissione.

Le autorità di sicurezza e i servizi competenti delle istituzioni dell'Unione possono effettuare, quale parte di un processo concordato avviato da una delle parti, valutazioni tra pari delle disposizioni di sicurezza per la protezione delle informazioni classificate scambiate a titolo dei pertinenti accordi interistituzionali.

10. **PROCEDURE DI DECLASSIFICAZIONE E DI RIMOZIONE DEL CONTRASSEGNO**

10.1. L'UIC esamina le informazioni classificate contenute nel suo registro e chiede il consenso dell'originatore per la declassificazione o la rimozione del contrassegno da un documento entro il 25° anno successivo alla data della sua creazione. I documenti non declassificati o a cui non è stato rimosso il contrassegno a seguito di un primo esame sono riesaminati periodicamente e comunque almeno ogni cinque anni. Oltre ad essere applicata ai documenti effettivamente conservati negli archivi protetti nella zona protetta e debitamente classificati, la procedura di rimozione del contrassegno può anche coprire le altre informazioni confidenziali conservate presso l'organo parlamentare/il titolare di un mandao o presso il servizio responsabile degli archivi storici del Parlamento.

10.2. La decisione relativa alla declassificazione o alla rimozione del contrassegno di un documento è, come regola generale, adottata unicamente dall'originatore o, in via eccezionale, in collaborazione con il servizio che detiene tali informazioni, prima che le informazioni che contiene siano trasmesse al servizio responsabile degli archivi storici del Parlamento. La declassificazione o la rimozione del contrassegno da informazioni classificate può essere effettuata unicamente previo accordo scritto dell'originatore. Nel caso delle «altre informazioni riservate», la segreteria dell'organo parlamentare/titolare di un mandato che detiene tali informazioni decide, in cooperazione con l'originatore, se si possa rimuovere il contrassegno dal documento.

10.3. L'UIC è tenuta a informare, per conto dell'originatore, i destinatari del documento del cambiamento di classificazione o di contrassegno e questi ultimi sono a loro volta tenuti a informarne i destinatari successivi ai quali hanno trasmesso l'originale o una copia del documento.

10.4. La declassificazione lascia impregiudicati eventuali ***indicazioni di sicurezza o*** contrassegni che possano figurare sul documento.

10.5. In caso di declassificazione, la classificazione originale figurante in cima e in fondo a ciascuna pagina è barrata. La prima pagina (pagina di copertina) del documento è vidimata e completata con il riferimento dell'UIC. In caso di rimozione del contrassegno, il contrassegno originale in cima a ciascuna pagina è barrato.

10.6. Il testo del documento declassificato o a cui è stato rimosso il contrassegno è allegato alla scheda elettronica o al sistema equivalente nel quale è stato registrato.

10.7. Nel caso di documenti coperti dalle eccezioni relative alla vita privata o all'integrità degli interessi privati o commerciali e nel caso di documenti sensibili si applica l'articolo 2 del regolamento del Consiglio (CEE, Euratom) n. 354/83.

10.8. Oltre alle disposizioni di cui ai punti da 10.1 a 10.7, si applicano le seguenti norme:

a) per quanto concerne i documenti di terzi, l'UIC consulta il terzo interessato prima di procedere alla declassificazione o alla rimozione del contrassegno;

b) per quanto concerne eccezioni relative alla vita privata e all'integrità dell'individuo, la procedura di declassificazione o di rimozione del contrassegno tiene conto in particolare del consenso della persona interessata o, all'occorrenza, dell'impossibilità di identificare la persona interessata;

c) per quanto concerne le eccezioni relative agli interessi commerciali di una persona fisica o giuridica, la persona interessata può essere informata mediante pubblicazione sulla *Gazzetta ufficiale dell'Unione europea* e dispone di un periodo di quattro settimane dal giorno della pubblicazione per presentare eventuali osservazioni.

Parte 2

PROCEDURA PER IL RILASCIO DEL NULLA OSTA DI SICUREZZA

11. **PROCEDURA PER IL RILASCIO DEL NULLA OSTA DI SICUREZZA AI DEPUTATI AL PARLAMENTO EUROPEO**

11.1. Per poter accedere alle informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente, i deputati al Parlamento europeo devono essere stati autorizzati secondo la procedura di cui ai punti 11.3 e 11.4 del presente allegato o in base a una dichiarazione solenne di non divulgazione a norma dell'articolo 3, paragrafo 4, della presente decisione.

11.2. Per poter accedere alle informazioni di livello «TRÈS SECRET UE/EU TOP SECRET» o «SECRET UE/EU SECRET» o equivalente, i deputati al Parlamento europeo devono essere stati autorizzati a tal fine secondo la procedura di cui ai punti 11.3 e 11.14.

11.3. L'autorizzazione è rilasciata soltanto ai deputati al Parlamento europeo che sono stati oggetto di un'indagine di sicurezza da parte delle autorità nazionali competenti degli Stati membri secondo la procedura di cui ai punti da 11.9 a 11.14. Il Presidente è responsabile del rilascio dell'autorizzazione ai deputati.

11.4. Il Presidente rilascia tale autorizzazione per iscritto previo parere delle autorità nazionali competenti degli Stati membri sulla base dell'indagine di sicurezza condotta conformemente ai punti da 11.8 a 11.13.

11.5. La direzione della sicurezza e della valutazione del rischio del Parlamento europeo tiene un elenco aggiornato di tutti i deputati al Parlamento europeo cui è stata rilasciata un'autorizzazione, compreso un'autorizzazione temporanea ai sensi del punto 11.4.

11.6. L'autorizzazione, che è valida per un periodo di cinque anni, o per la durata delle funzioni che ne hanno giustificato il rilascio, se più breve. Esso può essere rinnovato secondo la procedura di cui al punto 11.14.

11.7. L'autorizzazione è revocata dal Presidente ove questi ritenga che ve ne sia motivo. La decisione di revoca è notificata al deputato al Parlamento europeo interessato, che può chiedere di essere ascoltato dal Presidente prima che la revoca abbia effetto, nonché all'autorità nazionale competente.

11.8. L'indagine di sicurezza è effettuata con la collaborazione del deputato al Parlamento europeo interessato e su richiesta del Presidente. L'autorità nazionale competente è quella dello Stato membro di cui il deputato interessato è cittadino.

11.9. Ai fini dell'indagine di sicurezza, il deputato al Parlamento europeo interessato è tenuto a compilare un modulo informativo individuale.

11.10. Nella richiesta alle autorità nazionali competenti il Presidente specifica il livello di classificazione delle informazioni di cui il deputato al Parlamento europeo interessato dovrà prendere visione, per consentire loro di svolgere l'indagine di sicurezza.

11.11. Per lo svolgimento e i risultati della procedura relativa all'indagine di sicurezza svolta dalle autorità nazionali competenti si applicano le disposizioni e le norme vigenti in materia nello Stato membro interessato, comprese quelle relative agli eventuali mezzi di impugnazione.

11.12. Se l'autorità nazionale competente dello Stato membro esprime parere positivo, il Presidente può rilasciare l'autorizzazione al deputato al Parlamento europeo interessato.

11.13. Se l'autorità nazionale competente esprime parere negativo, il deputato al Parlamento europeo interessato è informato di tale parere e può chiedere di essere ascoltato dal Presidente. Il Presidente può, se lo ritiene necessario, rivolgersi all'autorità nazionale competente per chiarimenti complementari. In caso di riconferma del parere negativo, l'autorizzazione non può essere rilasciata.

11.14. I deputati al Parlamento europeo che abbiano ottenuto l'autorizzazione a norma del punto 11.3 ricevono, al momento del rilascio dell'autorizzazione e, successivamente, a intervalli regolari, le necessarie linee guida concernenti la protezione delle informazioni classificate e le modalità per garantirla. Tali deputati firmano una dichiarazione in cui confermano di avere ricevuto tali linee guida.

11.15. In via eccezionale, il Presidente, previa informazione dell'autorità nazionale competente e in mancanza di reazioni da parte di queste ultime entro il termine di un mese, può rilasciare a un deputato al Parlamento europeo un'autorizzazione temporanea per un periodo che non può essere superiore a sei mesi, in attesa dell'esito dell'indagine di cui al punto 11.11. Le autorizzazioni temporanee rilasciate non danno accesso alle informazioni di livello «TRÈS SECRET UE/EU TOP SECRET» o equivalente.

12. PROCEDURA PER IL RILASCIO DEL NULLA OSTA DI SICUREZZA AI FUNZIONARI DEL PARLAMENTO EUROPEO E ALTRI AGENTI IMPIEGATI PRESSO I GRUPPI POLITICI DEL PARLAMENTO

12.1. Hanno accesso alle informazioni classificate in possesso del Parlamento soltanto i funzionari del Parlamento europeo e gli altri agenti del Parlamento impiegati presso i gruppi politici i quali, a motivo delle loro funzioni e per esigenze di servizio, abbiano bisogno di prenderne visione o di effettuarne il trattamento.

12.2. Per poter accedere alle informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente, i funzionari del Parlamento europeo e gli altri agenti del Parlamento impiegati presso i gruppi politici devono essere stati autorizzati a tal fine secondo la procedura di cui ai punti 12.3 e 12.4.

12.3. L'autorizzazione è rilasciata soltanto alle persone di cui al punto 12.1 che sono state oggetto di un'indagine di sicurezza da parte delle autorità nazionali competenti degli Stati membri secondo la procedura di cui ai punti da 12.9 a 12.14. Il Segretario generale è responsabile del rilascio dell'autorizzazione ai funzionari del Parlamento europeo e altri agenti del Parlamento impiegati presso i gruppi politici.

12.4. Il Segretario generale può rilasciare per iscritto tale autorizzazione, previo parere delle autorità nazionali competenti degli Stati membri sulla base dell'indagine di sicurezza condotta conformemente ai punti da 12.8 a 12.13.

12.5. La direzione della sicurezza e della valutazione del rischio del Parlamento europeo tiene un elenco aggiornato di tutti i posti che richiedono un nulla osta di sicurezza, comunicati dai rispettivi servizi del Parlamento europeo, e di tutte le persone cui è stata rilasciata un'autorizzazione, anche temporanea.

12.6. L'autorizzazione è valida per un periodo di cinque anni, o per la durata delle funzioni che ne hanno giustificato il rilascio, se più breve. Essa può essere rinnovata secondo la procedura di cui al punto 12.4.

12.7. L'autorizzazione è revocata dal Segretario generale ove questi ritenga che ve ne sia motivo. La decisione di revoca è notificata al funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessato, che può chiedere di essere ascoltato dal Segretario generale prima che la revoca prenda effetto, nonché all'autorità nazionale competente.

12.8. L'indagine di sicurezza è effettuata con la collaborazione del funzionario del Parlamento europeo o dell'altro agente del Parlamento impiegato presso i gruppi politici interessato e su richiesta del Segretario generale. L'autorità nazionale competente è quella dello Stato membro di cui l'interessato è cittadino. Se consentito dalle disposizioni legislative e regolamentari nazionali, le autorità nazionali competenti possono condurre indagini sui cittadini stranieri che chiedono di consultare informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET».

12.9. Ai fini dell'indagine di sicurezza, il funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessato è tenuto a compilare un modulo informativo individuale.

12.10. Nella richiesta all'autorità nazionale competente il Segretario generale specifica il grado di classificazione delle informazioni di cui il funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessato dovrà prendere visione, per consentire all'autorità di svolgere l'indagine di sicurezza ed esprimere un parere in merito al grado di autorizzazione appropriato da accordare alla persona in questione.

12.11. Per lo svolgimento e i risultati della procedura relativa all'indagine di sicurezza svolta dall'autorità nazionale competente si applicano le disposizioni e le norme vigenti in materia nello Stato membro interessato, comprese quelle relative agli eventuali mezzi di impugnazione.

12.12. Se l'autorità nazionale competente dello Stato membro esprime parere positivo, il Segretario generale può accordare l'autorizzazione al funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessato.

12.13. Se l'autorità nazionale competente esprime parere negativo, il funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessato è informato di tale parere e può chiedere di essere ascoltato dal Segretario generale. Il Segretario generale può, se lo ritiene necessario, rivolgersi all'autorità nazionale competente per chiarimenti complementari. In caso di riconferma del parere negativo, l'autorizzazione non può essere rilasciata.

12.14. Ogni funzionario del Parlamento europeo e altro agente del Parlamento impiegato presso i gruppi politici che abbia ottenuto l'autorizzazione a norma dei punti 12.4 e 12.5 riceve, al momento del rilascio del medesimo e, successivamente, a intervalli regolari, le necessarie istruzioni concernenti la protezione delle informazioni classificate e le modalità per garantirla. Il funzionario o agente firma una dichiarazione in cui conferma di avere ricevuto tali istruzioni e di impegnarsi a rispettarle.

12.15. In via eccezionale, il Segretario generale, previa informazione dell'autorità nazionale competente e in mancanza di reazioni da parte di quest'ultima entro il termine di un mese, può rilasciare a un funzionario del Parlamento europeo o altro agente impiegato presso i gruppi politici un'autorizzazione temporanea per un periodo che non può essere superiore a sei mesi, in attesa dell'esito dell'indagine di sicurezza di cui al punto 12.11. Le autorizzazioni temporanee rilasciate non danno accesso alle informazioni di livello «TRÈS SECRET UE/EU TOP SECRET» o equivalente.

ALLEGATO II

INTRODUZIONE

Le presenti disposizioni disciplinano le comunicazioni di sicurezza che fissano e garantiscono la protezione in termini di trattamento e gestione delle informazioni riservate da parte del Parlamento europeo. Le comunicazioni di sicurezza costituiscono, unitamente alle istruzioni per il trattamento, il Sistema di gestione della sicurezza delle informazioni (Information Security Management System - ISMS) del Parlamento europeo di cui all'articolo 3, paragrafo 2, della presente decisione:

COMUNICAZIONE DI SICUREZZA 1

Organizzazione della sicurezza nel Parlamento europeo per quanto riguarda la protezione delle informazioni riservate

COMUNICAZIONE DI SICUREZZA 2

Gestione delle informazioni riservate

COMUNICAZIONE DI SICUREZZA 3

Trattamento delle informazioni riservate mediante i sistemi di comunicazione e informazione (CIS) automatizzati

COMUNICAZIONE DI SICUREZZA 4

Sicurezza materiale

COMUNICAZIONE DI SICUREZZA 5

Sicurezza industriale

COMUNICAZIONE DI SICUREZZA 6

Violazioni della sicurezza, perdita o compromissione di informazioni riservate

COMUNICAZIONE DI SICUREZZA 1

ORGANIZZAZIONE DELLA SICUREZZA NEL PARLAMENTO EUROPEO PER QUANTO RIGUARDA LA PROTEZIONE DELLE INFORMAZIONI RISERVATE

1. Il Segretario generale è responsabile dell'applicazione generale e coerente della presente decisione.

Il Segretario generale adotta tutte le misure necessarie per garantire che i deputati al Parlamento europeo, i funzionari del Parlamento europeo, gli agenti del Parlamento europeo che lavorano per i gruppi politici e i contraenti applichino la presente decisione negli edifici del Parlamento ai fini del trattamento o della conservazione delle informazioni riservate.

2. Il Segretario generale è l'autorità di sicurezza (AS), e in tale veste:

2.1. coordina tutte le questioni di sicurezza relative alle attività del Parlamento in relazione alla protezione delle informazioni riservate;

2.2. approva l'installazione di una zona protetta, di sale di lettura protette e di attrezzature protette;

2.3. attua le decisioni che autorizzano, ai sensi dell'articolo 6 della presente decisione, la trasmissione di informazioni classificate dal Parlamento a terzi;

2.4. indaga o ordina accertamenti su eventuali fughe di informazioni riservate avvenute *prima facie* nel Parlamento, d'intesa con il Presidente del Parlamento europeo, qualora sia interessato un deputato al Parlamento europeo;

2.5. intrattiene stretti contatti con le autorità di sicurezza delle altre istituzioni dell'Unione e con le autorità di sicurezza nazionale degli Stati membri, onde garantire un coordinamento ottimale della politica di sicurezza in materia di informazioni classificate;

2.6. verifica costantemente la politica e le procedure di sicurezza del Parlamento ed emette raccomandazioni appropriate che riflettono tale verifica;

2.7. riferisce all'autorità di sicurezza nazionale (ASN) che ha eseguito la procedura relativa all'indagine di sicurezza, conformemente all'allegato I, parte 2, punto 11.3, nei casi che riguardano qualsiasi informazione negativa che possa avere conseguenze per tale autorità.

3. Qualora sia interessato un deputato al Parlamento europeo, il Segretario generale lo solleva dagli incarichi in stretta collaborazione con il Presidente del Parlamento europeo.

4. Nell'adempimento dei propri compiti di cui ai paragrafi 2 e 3, il Segretario generale è assistito dal Segretario generale aggiunto, dalla direzione della sicurezza e della valutazione del rischio, dalla direzione delle tecnologie informatiche (DIT) e dall'unità informazioni classificate (UIC).

4.1. La direzione della sicurezza e della valutazione del rischio è responsabile delle misure di protezione personale e, in particolare, della procedura relativa al nulla osta di sicurezza, come disposto dall'allegato I, parte 2. La direzione della sicurezza e della valutazione del rischio, inoltre:

a) è il punto di contatto per le autorità di sicurezza delle altre istituzioni dell'Unione e per le ASN per quanto concerne le questioni relative alle procedure del nulla osta di sicurezza per i deputati al Parlamento, i funzionari del Parlamento europeo e gli agenti del Parlamento che lavorano per i gruppi politici;

b) fornisce le necessarie istruzioni generali di sicurezza sull'obbligo di proteggere le informazioni classificate e sulle conseguenze del mancato rispetto di tale obbligo;

c) vigila sul funzionamento della zona protetta e delle sale di lettura protette all'interno degli edifici del Parlamento, in collaborazione, se del caso, con i servizi di sicurezza delle altre istituzioni dell'Unione e delle ASN;

d) controlla, in collaborazione con le autorità di sicurezza delle altre istituzioni dell'Unione e delle ASN, le procedure in materia di gestione e conservazione delle informazioni classificate, la zona protetta e le sale di lettura protette all'interno degli edifici del Parlamento in cui vengono trattate le informazioni classificate;

e) propone al Segretario generale le necessarie istruzioni per il trattamento.

4.2. La DIT è responsabile del trattamento di informazioni riservate mediante sistemi di sicurezza informatici al Parlamento europeo.

4.3. All'UIC compete:

a) l'individuazione delle esigenze di sicurezza per un'effettiva protezione delle informazioni riservate, in stretta collaborazione con la direzione della sicurezza e della valutazione del rischio e la DIT e con le autorità di sicurezza delle altre istituzioni dell'Unione;

b) l'individuazione di tutti gli aspetti inerenti alla gestione e alla conservazione delle informazioni riservate all'interno del Parlamento, come stabilito nelle istruzioni per il trattamento;

c) il funzionamento della zona protetta;

d) la gestione o consultazione delle informazioni riservate nella zona protetta o nella sala di lettura protetta dell'UIC, conformemente all'articolo 7, paragrafi 2 e 3, della presente decisione;

e) la gestione del registro dell'UIC;

f) la comunicazione all'AS di qualsiasi violazione, comprovata o sospetta, della sicurezza, perdita o compromissione di informazioni riservate custodite nell'UIC e detenute nella zona protetta o nella sala di lettura protetta dell'UIC.

5. Il Segretario generale provvede inoltre, in qualità di AS, a nominare le autorità seguenti:

a) un'autorità di accreditamento di sicurezza (SAA);

b) un'autorità operativa per la garanzia di sicurezza delle informazioni (IAOA);

c) un'autorità di distribuzione degli apparati crittografici (CDA);

d) un'autorità TEMPEST (TA);

e) un'autorità per la garanzia di sicurezza delle informazioni (IAA);

L'esercizio di tali funzioni non richiede entità organizzative uniche. I mandati sono specifici, anche se le funzioni, e le responsabilità ad esse collegate, possono combinarsi o integrarsi nella stessa entità organizzativa o suddividersi tra diverse entità organizzative, a condizione che si evitino conflitti di interesse e duplicazioni di mansioni.

6. La SAA fornisce pareri su tutte le questioni di sicurezza connesse all'accreditamento, in seno al Parlamento, di ogni sistema e rete relativi alle tecnologie informatiche, e provvede:

6.1. assicurando che il CIS sia conforme alle politiche e agli orientamenti di sicurezza pertinenti, fornendo una dichiarazione di approvazione per il trattamento da parte del CIS di informazioni classificate a un determinato livello di classificazione nel suo contesto operativo, e specificando i termini e le condizioni di accreditamento e i criteri in base ai quali è richiesta una nuova approvazione;

6.2. istituendo una procedura di accreditamento di sicurezza, conformemente alle pertinenti politiche, che definisca chiaramente le condizioni per l'approvazione dei CIS rientranti sotto la sua autorità;

6.3. a elaborare una strategia di accreditamento di sicurezza che definisca il livello di dettaglio del processo di accreditamento commisurandolo al livello di garanzia richiesto;

6.4. a esaminare e approvare la documentazione attinente alla sicurezza, comprese le dichiarazioni di gestione del rischio e quelle sul rischio residuo, la documentazione relativa alla verifica dell'attuazione della sicurezza e le procedure operative di sicurezza, garantendone la conformità alle norme e alle politiche di sicurezza del Parlamento;

6.5. a controllare l'attuazione delle misure di sicurezza in relazione al CIS effettuando direttamente o finanziando valutazioni, ispezioni o riesami riguardo alla sicurezza;

6.6. a individuare i requisiti di sicurezza (ad es. livelli di nulla osta personale) per i posti sensibili in relazione al CIS;

6.7. ad approvare l'interconnessione ad altri CIS di un CIS o, se del caso, partecipare all'approvazione congiunta di tale interconnessione;

6.8. ad approvare le norme di sicurezza delle attrezzature tecniche destinate al trattamento sicuro e alla protezione delle informazioni classificate;

6.9. garantire che i prodotti crittografici utilizzati all'interno del Parlamento siano inclusi nell'elenco dei prodotti approvati dall'UE; nonché

6.10. a consultare il fornitore del sistema, gli operatori della sicurezza e i rappresentanti degli utenti per quanto riguarda la gestione del rischio di sicurezza, in particolare il rischio residuo, nonché i termini e le condizioni della dichiarazione di approvazione.

7. L'IAOA ha il compito di:

7.1. sviluppare una documentazione di sicurezza che sia conforme alle politiche e agli orientamenti di sicurezza, compresi, in particolare, la dichiarazione sul rischio residuo, le procedure operative di sicurezza e il piano crittografico nell'ambito del processo di accreditamento del CIS;

7.2. partecipare alla selezione e alla verifica di misure, dispositivi e software di sicurezza tecnica specifici del sistema, per sorvegliarne l'attuazione e assicurarne l'installazione, la configurazione e la manutenzione in modo sicuro conformemente alla relativa documentazione di sicurezza;

7.3. controllare l'attuazione e l'applicazione delle procedure operative di sicurezza e, ove opportuno, delegare le responsabilità di sicurezza operativa al proprietario del sistema, in particolare l'UIC;

7.4. gestire e trattare prodotti crittografici, assicurando la custodia di apparati crittografici e controllati e, se richiesto, garantire la produzione di variabili crittografiche;

7.5. svolgere analisi, esami e verifiche di sicurezza, in particolare al fine di elaborare le pertinenti relazioni sui rischi, come richiesto dalla SAA;

7.6. fornire una formazione sulla garanzia delle informazioni specifica del CIS;

7.7. attuare e mettere in funzione misure di sicurezza specifiche del CIS.

8. La CDA ha il compito di:

8.1. gestire e rendere conto del materiale crittografico dell'UE;

8.2. assicurare, in stretta collaborazione con la SAA, che siano attuate procedure appropriate e siano stabiliti piani per rendere conto di tutto il materiale crittografico dell'UE e assicurarne il trattamento, la conservazione e la diffusione in modo sicuro; nonché

8.3. assicurare il trasferimento di materiale crittografico dell'UE verso o da singoli individui o servizi che lo utilizzano.

9. L'a TA è responsabile della conformità dei CIS con le politiche e le istruzioni in materia di trattamento TEMPEST. Essa approva le contromisure TEMPEST per le installazioni e i prodotti per proteggere le informazioni classificate a un determinato livello di classifica nel suo contesto operativo.

10. L'IAA è responsabile di tutti gli aspetti inerenti alla gestione e al trattamento delle informazioni riservate all'interno del Parlamento e, in particolare, ha il compito di:

10.1 sviluppare la sicurezza della garanzia delle informazioni e i suoi orientamenti di sicurezza, monitorando la loro efficacia e pertinenza;

10.2. salvaguardare e gestire informazioni tecniche relative ai prodotti crittografici;

10.3. garantire che le misure in materia di garanzia delle informazioni, adottate per proteggere le informazioni classificate, rispettino le politiche pertinenti che ne disciplinano l'ammissibilità e la selezione;

10.4. garantire che i prodotti crittografici siano selezionati nel rispetto delle politiche che ne disciplinano l'ammissibilità e la selezione;

10.5. consultare il fornitore del sistema, gli operatori della sicurezza e i rappresentanti degli utenti per quanto riguarda la sicurezza in materia di garanzia delle informazioni.

COMUNICAZIONE DI SICUREZZA 2

GESTIONE DELLE INFORMAZIONI RISERVATE

A. **INTRODUZIONE**

1. La presente comunicazione di sicurezza stabilisce le disposizioni relative alla gestione, da parte del Parlamento, delle informazioni riservate.

2. All'atto della creazione di informazioni riservate, l'originatore valuta il livello di riservatezza e decide se procedere alla classificazione delle informazioni in esame o all'apposizione di un contrassegno conformemente ai principi stabiliti nella presente comunicazione di sicurezza.

B. **CLASSIFICAZIONE ICUE**

3. La decisione relativa alla classificazione o meno di un documento è presa prima della sua creazione. A tal fine, la classificazione di informazioni come ICUE prevede una valutazione preliminare del livello di riservatezza delle stesse e una decisione dell'originatore che stabilisca che la divulgazione non autorizzata delle informazioni in questione recherebbe in varia misura pregiudizio agli interessi dell'Unione europea oppure di uno o più Stati membri o persone fisiche.

4. Una volta presa la decisione di classificare le informazioni, viene effettuata una seconda valutazione preliminare intesa a determinare l'opportuno livello di classificazione. La classificazione di un documento è determinata dal livello di sensibilità del suo contenuto.

5. La responsabilità della classificazione delle informazioni spetta unicamente all'originatore. I funzionari del Parlamento classificano le informazioni su istruzione o per delega del Segretario generale.

6. La classificazione è attribuita correttamente e con moderazione. L'originatore di un documento che deve essere classificato limita la tendenza alla sovraclassificazione o alla sottoclassificazione.

7. Il livello di classificazione assegnato alle informazioni determina il livello di protezione ad esse attribuito negli ambiti della sicurezza del personale, della sicurezza materiale, della sicurezza procedurale e della garanzia di sicurezza delle informazioni.

8. Le informazioni che richiedono la classificazione sono contrassegnate e trattate in quanto informazioni classificate a prescindere dalla loro forma fisica. La classificazione è comunicata in modo chiaro ai destinatari, mediante un contrassegno di classificazione di sicurezza (qualora le informazioni siano comunicate per iscritto, per esempio su carta o nell'ambito del CIS) o mediante un annuncio (qualora le informazioni siano comunicate oralmente, per esempio nell'ambito di una conversazione o di una riunione a porte chiuse). Il materiale classificato deve essere contrassegnato fisicamente in modo che la classificazione di sicurezza possa essere facilmente individuata.

9. Le ICUE in formato elettronico possono essere create soltanto in CIS accreditati. Il pertinente contrassegno di classificazione di sicurezza è apposto sulle informazioni classificate stesse così come sul nome del file e sull'unità di memoria (se esterna, ad es. CD-ROM o chiave USB).

10. Le informazioni sono classificate al momento della loro creazione. Per esempio, le note personali, i progetti o i messaggi di posta elettronica contenenti informazioni che richiedono una classificazione devono essere contrassegnati fin dall'inizio come ICUE ed essere elaborati e trattati dal punto di vista materiale e tecnico in conformità della presente decisione e delle istruzioni relative al trattamento. Queste informazioni possono quindi trasformarsi in un documento ufficiale che a sua volta sarà contrassegnato e trattato in modo appropriato. È possibile che, nel corso del processo di elaborazione, un documento ufficiale debba essere sottoposto a una nuova valutazione e che la sua evoluzione giustifichi un livello di classificazione superiore o inferiore.

11. Gli originatori possono decidere di attribuire un livello di classificazione standard a determinate categorie di informazioni da essi create regolarmente. In tal caso devono tuttavia fare in modo di evitare la sovraclassificazione o la sottoclassificazione sistematica di determinate informazioni.

12. Le ICUE recano sempre un contrassegno di classificazione di sicurezza corrispondente al loro livello di classificazione di sicurezza.

B.1. ***Livelli di classificazione***

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

— «TRÈS SECRET UE/EU TOP SECRET», ai sensi dell'articolo 2, lettera d), della presente decisione, qualora la compromissione delle informazioni possa:

a) minacciare direttamente la stabilità interna dell'Unione, di uno o più Stati membri, di Stati terzi oppure di organizzazioni internazionali;

b) causare danni di eccezionale gravità alle relazioni con Stati terzi o organizzazioni internazionali;

c) provocare direttamente la perdita di molte vite umane;

d) occasionare danni di eccezionale gravità all'efficacia operativa o alla sicurezza del personale dispiegato degli Stati membri o di altri contributori ovvero all'ininterrotta efficacia di operazioni di sicurezza o di intelligence di massima rilevanza;

e) arrecare gravi danni a lungo termine all'economia dell'Unione o degli Stati membri;

— «SECRET UE/EU SECRET», ai sensi dell'articolo 2, lettera d), della presente decisione, qualora la compromissione delle informazioni possa:

a) incrementare in misura significativa le tensioni internazionali;

b) danneggiare seriamente le relazioni con Stati terzi e organizzazioni internazionali;

c) costituire una minaccia diretta di perdita di vite umane o un grave pregiudizio all'ordine pubblico o alla sicurezza o libertà individuali;

d) danneggiare importanti negoziati commerciali o politici; creare seri problemi operativi per l'Unione o gli Stati membri;

e) arrecare gravi danni alla sicurezza operativa degli Stati membri o all'efficacia di operazioni di sicurezza o di intelligence di grande rilevanza;

f) causare ingenti danni materiali agli interessi finanziari, monetari, economici e commerciali dell'Unione o degli Stati membri;

g) compromettere in modo sostanziale la capacità finanziaria di grandi operatori o organizzazioni; oppure

h) ostacolare in modo significativo l'elaborazione o l'attuazione delle politiche dell'Unione con gravi ripercussioni economiche, commerciali o finanziarie;

— «CONFIDENTIEL UE/EU CONFIDENTIAL», ai sensi dell'articolo 2, lettera d), della presente decisione, qualora la compromissione delle informazioni possa:

a) danneggiare gravemente le relazioni diplomatiche, ad esempio portando a una protesta formale o ad altre sanzioni;

b) mettere a repentaglio la sicurezza o la libertà individuali;

c) mettere gravemente a rischio l'esito di negoziati commerciali o politici; creare problemi operativi per l'Unione o per uno o più Stati membri;

d) danneggiare la sicurezza operativa degli Stati membri o l'efficacia di operazioni di sicurezza o di intelligence;

e) compromettere in modo sostanziale la capacità finanziaria di grandi operatori o organizzazioni;

f) ostacolare le indagini o facilitare i reati o le attività terroristiche;

g) andare gravemente a discapito degli interessi finanziari, monetari, economici e commerciali dell'Unione o degli Stati membri; o

h) ostacolare in modo significativo l'elaborazione o l'attuazione delle politiche dell'Unione con gravi ripercussioni economiche, commerciali o finanziarie;

— «RESTREINT UE/EU RESTRICTED», ai sensi dell'articolo 2, lettera d), della presente decisione, qualora la compromissione delle informazioni possa:

a) andare a discapito degli interessi generali dell'Unione;

b) ripercuotersi negativamente sulle relazioni diplomatiche;

c) creare notevoli difficoltà per individui o imprese;

d) andare a discapito dell'Unione o degli Stati membri nel quadro di negoziati commerciali o politici;

e) rendere più difficile l'efficace mantenimento della sicurezza all'interno dell'Unione o degli Stati membri;

f) ostacolare l'efficace elaborazione o attuazione delle politiche dell'Unione;

g) compromettere la corretta gestione dell'Unione e delle sue operazioni;

h) violare l'impegno del Parlamento di mantenere la riservatezza delle informazioni classificate fornite da terzi;

i) violare i vincoli regolamentari relativi alla divulgazione di informazioni;

j) causare perdite finanziarie o facilitare i profitti o i vantaggi indebiti per singoli individui e società; oppure

k) pregiudicare le indagini o facilitare i reati.

B.2. ***Classificazione delle compilazioni, delle pagine di copertina e degli estratti***

14. Il livello di classificazione attribuito a una lettera o nota cui è accluso altro materiale corrisponde a quello dell'elemento accluso di livello più elevato. L'originatore indica chiaramente il livello di classificazione da attribuire alla lettera o nota quando è separata dal materiale accluso. Qualora la nota/lettera di accompagnamento non richieda una classificazione, è apposta la seguente dicitura finale: «Quando è separata dal materiale accluso, la presente nota/lettera non è classificata».

15. I documenti o file che contengono componenti caratterizzati da livelli di classificazione diversi devono essere impostati, ogniqualvolta possibile, in modo che i componenti con un livello di classificazione diverso possano essere facilmente individuati e, se necessario, separati. Il livello di classificazione generale di un documento o file corrisponde come minimo a quello del suo componente di livello più elevato.

16 È possibile che singole pagine, paragrafi, sezioni, annessi, appendici o allegati di un determinato documento e altro materiale accluso richiedano livelli di classificazione differenti, nel qual caso detti elementi sono classificati di conseguenza. Nei documenti contenenti ICUE è possibile utilizzare abbreviazioni standard per indicare il livello di classificazione di sezioni o blocchi di testo di lunghezza inferiore a una pagina.

17. Quando si riprendono informazioni da varie fonti, il prodotto finale è riesaminato per determinarne il livello generale di classificazione di sicurezza, in quanto può richiedere una classificazione più elevata di quella dei suoi componenti.

C. **ALTRE INFORMAZIONI RISERVATE**

18. Le «altre informazioni riservate» sono contrassegnate in conformità della lettera E della presente comunicazione di sicurezza e delle istruzioni relative al trattamento.

D. **CREAZIONE DI INFORMAZIONI RISERVATE**

19. Possono creare informazioni riservate solo le persone debitamente legittimate dalla presente decisione o autorizzate dall'AS.

20. Le informazioni riservate non sono inserite in sistemi di gestione dei documenti su Internet o Intranet.

D.1. ***Creazione di ICUE***

21. Per poter creare ICUE classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», la persona interessata deve essere legittimata dalla presente decisione o essere in possesso di un'autorizzazione preliminare rilasciata a norma dell'articolo 4, paragrafo 1, della presente decisione.

22. Le ICUE classificate come «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» sono create esclusivamente all'interno della zona protetta.

23. La creazione di ICUE è disciplinata dalle norme seguenti:

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

b) ciascuna pagina è numerata e reca l'indicazione del numero totale di pagine;

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

d) il documento è datato sulla prima pagina;

e) sulla prima pagina di tutti i documenti classificati di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» è indicato un elenco di tutti gli allegati e i materiali acclusi;

f) i documenti classificati di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» recano su ogni pagina l'indicazione del numero della copia, se devono essere distribuiti in più copie; sulla prima pagina di ogni copia è inoltre indicato il numero totale delle copie e delle pagine;

g) se il documento fa riferimento ad altri documenti contenenti informazioni classificate ricevuti da altre istituzioni dell'Unione, oppure include informazioni classificate derivanti da tali documenti, è soggetto allo stesso livello di classificazione dei documenti in questione e non può, in assenza di un'autorizzazione preliminare scritta del suo originatore, essere distribuito a persone diverse da quelle specificate nella lista di distribuzione relativa al documento o ai documenti originali contenenti informazioni classificate.

24. Le ICUE restano sotto il controllo dell'originatore che le ha create. È necessario ottenere la sua autorizzazione preliminare scritta prima che le ICUE possano essere:

a) declassate o declassificate;

b) utilizzate a fini diversi da quelli stabiliti dall'originatore;

c) rivelate a qualsiasi Stato terzo o organizzazione internazionale;

d) rivelate a qualsiasi persona, istituzione, paese o organizzazione internazionale che non rientri tra i destinatari che l'originatore aveva inizialmente autorizzato a consultare le informazioni in questione;

e) rivelate a un contraente o a un potenziale contraente situato in uno Stato terzo;

f) copiate o tradotte, se le informazioni sono classificate di livello «TRÈS SECRET UE/EU TOP SECRET»;

g) distrutte.

D.2. ***Creazione di altre informazioni riservate***

25. Il Segretario generale agendo in qualità di AS può decidere se autorizzare o meno la creazione di «altre informazioni riservate» da parte di una data funzione, un dato servizio e/o soggetto.

26. Le «altre informazioni riservate» recano uno dei contrassegni definiti nelle istruzioni relative al trattamento.

27. La creazione di «altre informazioni riservate» è disciplinata dalle norme seguenti:

a) il relativo contrassegno è indicato in cima alla prima pagina del documento;

b) ciascuna pagina è numerata e reca l'indicazione del numero totale di pagine;

c) il documento reca un numero di riferimento sulla prima pagina e un'indicazione del suo oggetto;

d) il documento è datato sulla prima pagina;

e) l'ultima pagina del documento contiene un elenco di tutti gli allegati e i materiali acclusi.

28. La creazione di «altre informazioni riservate» è disciplinata da specifiche norme e procedure stabilite nelle istruzioni relative al trattamento.

E. **INDICAZIONI DI SICUREZZA E CONTRASSEGNI**

29. Le indicazioni di sicurezza e i contrassegni sui documenti sono destinati a controllare il flusso delle informazioni e a limitare l'accesso alle informazioni riservate sulla base del principio della necessità di sapere.

30. Quando si utilizzano o si appongono indicazioni di sicurezza e/o contrassegni, si cura di evitare confusione con le classificazioni di sicurezza per le ICUE: « RESTREINT UE/EU RESTRICTED», «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET», «TRES SECRET UE/EU TOP SECRET».

31. Nelle istruzioni relative al trattamento si stabiliscono le norme specifiche concernenti l'uso di indicazioni di sicurezza e contrassegni, unitamente all'elenco dei contrassegni di sicurezza del Parlamento europeo approvati.

E.1. ***Indicazioni di sicurezza***

32. Le indicazioni di sicurezza possono essere utilizzate soltanto in combinazione con una classificazione di sicurezza e non sono applicate separatamente ai documenti. Un'indicazione di sicurezza può essere applicata alle ICUE al fine di:

a) porre limiti alla validità di una classificazione (per il declassamento o la declassificazione automatica di informazioni classificate);

b) limitare la distribuzione delle ICUE in questione;

c) stabilire modalità specifiche di trattamento oltre a quelle corrispondenti al livello della classificazione di sicurezza.

33. I controlli aggiuntivi applicabili al trattamento e alla conservazione di documenti contenenti ICUE impongono oneri supplementari a tutti i soggetti coinvolti. Per ridurre al minimo le attività necessarie in tal senso, è buona prassi, al momento della creazione di tali documenti, stabilire un limite di tempo o un evento dopo il quale la classificazione decade automaticamente e le informazioni contenute nel documento sono declassate o declassificate.

34. Qualora un documento riguardi uno specifico settore di attività e sia necessario limitarne la distribuzione e/o osservare modalità specifiche di trattamento, è possibile aggiungere alla sua classificazione una dichiarazione a tal fine, per contribuire a identificare i relativi destinatari.

E.2. ***Contrassegni***

35. I contrassegni non costituiscono una classificazione di sicurezza. Essi sono destinati unicamente a fornire istruzioni concrete riguardanti il trattamento di un documento e non sono utilizzati per descrivere il contenuto di tale documento.

36. I contrassegni possono essere apposti separatamente ai documenti o utilizzati unitamente a una classificazione di sicurezza.

37. Di norma, i contrassegni si applicano alle informazioni che sono coperte dal segreto professionale di cui all'articolo 339 TFUE e all'articolo 17 dello statuto dei funzionari, o che devono essere protette dal Parlamento per ragioni giuridiche, ma che non devono, o non possono essere classificate.

E.3. ***Uso dei contrassegni presso il CIS***

38. Le norme relative all'uso dei contrassegni sono applicabili anche presso i CIS accreditati.

39. La SAA stabilisce norme specifiche riguardanti l'uso dei contrassegni presso i CIS accreditati.

F. **RICEZIONE DELLE INFORMAZIONI**

40. Solo l'UIC è autorizzato all'interno del Parlamento a ricevere informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» o di livello equivalente, da parte di terzi.

41. Per quanto concerne le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate», sia l'UIC che il competente organo parlamentare/titolare di un mandato possono avere il compito di riceverle da terzi e di applicare i principi stabiliti nella presente comunicazione di sicurezza.

G. **REGISTRAZIONE**

42. Per registrazione si intende l'applicazione di procedure che consentono di registrare il ciclo di vita di informazioni riservate, comprese la loro diffusione, consultazione e distruzione.

43. Ai fini della presente comunicazione di sicurezza, per «repertorio» si intende un registro che riporta in particolare la data e l'ora in cui un'informazione riservata:

a) raggiunge o lascia la rispettiva segreteria dell'organo parlamentare/del titolare di un mandato oppure, a seconda dei casi, l'UIC;

b) viene trasmessa a una persona munita di nulla osta di sicurezza o quando questa vi accede; e

c) viene distrutta.

44. L'originatore di informazioni riservate ha il compito di contrassegnare la dichiarazione iniziale al momento della creazione di un documento contenente tali informazioni. Tale dichiarazione è comunicata all'UIC quando il documento viene creato.

45. Le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, possono unicamente essere registrate dall'UIC a fini di sicurezza. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate» ricevute da terzi sono registrate dal servizio responsabile della ricezione ufficiale del documento, ovvero l'UIC oppure la segreteria dell'organo parlamentare/del titolare di un mandato, ai fini amministrativi. Le «altre informazioni riservate» prodotte all'interno del Parlamento sono registrate dall'originatore, ai fini amministrativi.

46. Le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, sono registrate in particolare quando:

a) sono prodotte;

b) raggiungono o lasciano l'UIC; e

c) raggiungono o lasciano il CIS.

47. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o di livello equivalente sono registrate in particolare quando:

a) sono prodotte;

b) raggiungono o lasciano la rispettiva segreteria dell'organo parlamentare/del titolare di un mandato oppure l'UIC; e

c) raggiungono o lasciano il CIS.

48. La registrazione delle informazioni riservate può essere effettuata mediante un repertorio cartaceo o elettronico/in un CIS.

49. Per le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate», si registra almeno quanto segue:

a) la data e l'ora in cui raggiungono o lasciano la rispettiva segreteria dell'organo parlamentare/del titolare di un mandato oppure l'UIC, a seconda dei casi;

b) il titolo del documento, il livello di classificazione o il contrassegno, la data di scadenza della classificazione/del contrassegno e l'eventuale numero di riferimento assegnato al documento.

50. Per le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, si registra almeno quanto segue:

a) la data e l'ora in cui raggiungono o lasciano l'UIC;

b) il titolo del documento, il livello di classificazione o il contrassegno, l'eventuale numero di riferimento assegnato al documento e la data di scadenza della classificazione/del contrassegno;

c) i dati personali dell'originatore;

d) l'identità delle persone che hanno diritto ad accedere al documento e la data in cui tali persone ha avuto accesso al documento;

e) le eventuali copie o traduzioni del documento;

f) la data e l'ora in cui eventuali copie o traduzioni del documento lasciano l'UIC o vi ritornano, nonché il recapito al quale sono state inviate e i dati di chi le ha restituite;

g) la data e l'ora in cui il documento è distrutto e da chi, conformemente alle norme di sicurezza del Parlamento in materia di distruzione; e

h) il declassamento o la declassificazione del documento.

51. I repertori sono classificati o contrassegnati in modo adeguato. I repertori per le informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente sono registrati allo stesso livello.

52. Le informazioni classificate possono essere registrate:

a) in un unico repertorio; o

b) in repertori separati a seconda del livello di classificazione, del fatto che si tratti di informazioni in entrata o in uscita nonché della loro origine o destinazione.

53. Nel caso di trattamento elettronico nell'ambito del CIS, le procedure di registrazione possono essere svolte all'interno del CIS stesso con mezzi conformi a requisiti equivalenti a quelli sopra specificati. Quando le ICUE lasciano il perimetro del CIS, si applica la procedura di registrazione di cui sopra.

54. L'UIC tiene un registro di tutte le informazioni classificate comunicate dal Parlamento a terzi e delle informazioni classificate che il Parlamento ha ricevuto da terzi.

55. Una volta completata la registrazione di informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, l'UIC verifica se il destinatario dispone di un'autorizzazione di sicurezza valida. In caso affermativo, l'UIC notifica il destinatario. La consultazione delle informazioni classificate è possibile soltanto dopo la registrazione del documento che le contiene.

H. **DISTRIBUZIONE**

56. L'originatore stabilisce la lista di distribuzione iniziale per le ICUE che ha creato.

57. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» e altre informazioni riservate prodotte dal Parlamento sono distribuite all'interno del Parlamento dall'originatore, conformemente alle pertinenti istruzioni di trattamento e sulla base del principio della necessità di sapere. Per le informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», create dal Parlamento all'interno della zona protetta, la lista di distribuzione (ed eventuali ulteriori istruzioni concernenti la distribuzione) è fornita all'UIC, che è responsabile di gestirla.

58. Le ICUE prodotte dal Parlamento possono essere distribuite a terzi soltanto dall'UIC, sulla base del principio della necessità di sapere.

59. Le informazioni riservate ricevute dall'UIC o da un organo parlamentare/titolare di un mandato che ne ha fatto richiesta sono distribuite conformemente alle istruzioni ricevute dall'originatore.

I. **TRATTAMENTO, CONSERVAZIONE E CONSULTAZIONE**

60. Il trattamento, la conservazione e la consultazione delle informazioni riservate avvengono conformemente alla comunicazione di sicurezza 4 e alle istruzioni di trattamento.

J. **COPIA/TRADUZIONE/INTERPRETAZIONE DI INFORMAZIONI CLASSIFICATE**

61. I documenti contenenti informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente possono essere copiati o tradotti solo previo consenso scritto dell'originatore. I documenti contenenti informazioni classificate di livello «SECRET UE/EU SECRET» o equivalente, o di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente possono essere copiati o tradotti su istruzione del detentore, purché l'originatore non l'abbia vietato.

62. Ogni copia di un documento contenente informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET», «SECRET UE/EU SECRET» o «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente è registrata ai fini di sicurezza.

63. Le misure di sicurezza applicabili al documento originale contenente informazioni classificate si applicano alle relative copie e traduzioni.

64. I documenti ricevuti dal Consiglio devono essere in tutte le lingue ufficiali.

65. Copie e/o traduzioni di documenti contenenti informazioni classificate possono essere richieste dall'originatore o dal detentore di una copia. Le copie di documenti contenenti informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, possono essere prodotte soltanto nella zona protetta e mediante fotocopiatrici appartenenti a un CIS accreditato. Le copie di documenti contenenti informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e altre informazioni riservate sono effettuate mediante un dispositivo di riproduzione accreditato all'interno dei locali del Parlamento.

66. Tutte le copie e le traduzioni di documenti, o parti di copie di documenti, contenenti informazioni riservate, sono appositamente contrassegnate, numerate e registrate.

67. Si effettuano soltanto le copie strettamente necessarie. Tutte le copie vengono distrutte conformemente alle istruzioni di trattamento al termine del periodo di consultazione.

68. Soltanto gli interpreti e i traduttori che sono funzionari del Parlamento hanno accesso alle informazioni classificate.

69. Gli interpreti e i traduttori che hanno accesso a documenti contenenti informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente, hanno l'apposito nulla osta di sicurezza.

70. Gli interpreti e i traduttori lavorano all'interno della zona protetta quando si occupano di documenti contenenti informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o di livello equivalente.

K. **DECLASSAMENTO, DECLASSIFICAZIONE E RIMOZIONE DEL CONTRASSEGNO DI INFORMAZIONI RISERVATE**

K.1. ***Principi generali***

71. Le informazioni riservate sono declassificate o declassate, o si rimuove il loro contrassegno, quando la protezione non è più necessaria o non è necessaria al livello iniziale.

72. Le decisioni di declassamento, declassificazione o rimozione del contrassegno di informazioni contenute in documenti elaborati all'interno del Parlamento possono anche essere prese caso per caso, ad esempio, in risposta a una richiesta di accesso del pubblico o di un'altra istituzione dell'Unione, o su iniziativa dell'UIC o dell'organo parlamentare/del titolare di un mandato.

73. Al momento della creazione delle ICUE l'originatore indica, laddove possibile, se queste possono essere declassate o declassificate a una certa data o in seguito a un dato evento. Quando non sia possibile fornire tale indicazione, l'originatore, l'UIC o l'organo parlamentare/il titolare di un mandato che è in possesso delle informazioni rivede il livello di classificazione delle ICUE almeno una volta ogni cinque anni. In ogni caso, le ICUE possono essere declassate o declassificate solo previo consenso scritto dell'originatore.

74. Nel caso in cui non sia possibile determinare o individuare l'originatore delle ICUE relative a documenti elaborati all'interno del Parlamento, l'AS rivede il livello di classificazione delle ICUE in questione sulla base di una proposta dell'organo parlamentare/del titolare di un mandato che è in possesso delle informazioni, il quale può consultare l'UIC a tale riguardo.

75. L'UIC o l'organo parlamentare/il titolare di un mandato che è in possesso delle informazioni è responsabile di notificare ai destinatari che le informazioni sono state declassificate o declassate, e i destinatari sono a loro volta tenuti a notificare i destinatari successivi ai quali hanno trasmesso l'originale o una copia del documento.

76. La declassificazione, il declassamento o la rimozione del contrassegno di informazioni contenute in un documento devono essere registrati.

K.2. ***Declassificazione***

77. Le ICUE possono essere declassificate integralmente o in parte. Esse possono essere parzialmente declassificate quanto la protezione non è più ritenuta necessaria per una data parte del documento che le contiene, ma continua a essere giustificata per il resto del documento.

78. Quando la revisione delle ICUE contenute in un documento elaborato all'interno del Parlamento si conclude con la decisione di declassificarle, occorre valutare se il documento possa essere reso pubblico o debba recare un contrassegno di distribuzione (vale a dire, che non sia reso pubblico).

79. Quando le ICUE sono declassificate, la loro declassificazione è registrata in un repertorio con i seguenti dati: la data di declassificazione, i nomi delle persone che hanno richiesto e che hanno autorizzato la declassificazione, il numero di riferimento del documento declassificato e la sua destinazione finale.

80. I vecchi contrassegni di classificazione devono essere barrati nel documento declassificato e in tutte le sue copie. Il documento originale e tutte le sue copie sono archiviati di conseguenza.

81. Dopo una declassificazione parziale di informazioni classificate, si produce un estratto della parte declassificata, che viene adeguatamente archiviato. Il servizio competente registra:

a) la data della declassificazione parziale;

b) i nomi delle persone che hanno richiesto e che hanno autorizzato la declassificazione; e

c) il numero di riferimento dell'estratto declassificato.

K.3. ***Declassamento***

82. In seguito al declassamento di informazioni classificate, il documento in cui sono contenute è registrato nei repertori che corrispondono al vecchio e al nuovo livello di classificazione. Si registrano la data del declassamento e il nome della persona che l'ha autorizzato.

83. Il documento contenente le informazioni declassate e tutte le sue copie sono classificati con il nuovo livello di classificazione e adeguatamente archiviati.

L. **DISTRUZIONE DI INFORMAZIONI RISERVATE**

84. Le informazioni riservate (in formato cartaceo o elettronico) che non sono più necessarie vengono distrutte o cancellate, in base alle istruzioni di trattamento e ai regolamenti pertinenti in materia di archiviazione.

85. Le informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o «SECRET UE/EU SECRET» o equivalente, sono distrutte dall'UIC. La loro distruzione avviene in presenza di un testimone titolare di un nulla osta di sicurezza corrispondente almeno al livello di classificazione dell'informazione che viene distrutta.

86. Le informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente possono essere distrutte solo previo consenso scritto dell'originatore.

87. Le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» o equivalente sono distrutte ed eliminate dall'UIC sulla base delle istruzioni dell'originatore o di un'autorità competente. I repertori e gli altri registri sono aggiornati di conseguenza. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente sono distrutte ed eliminate dall'UIC o dal pertinente organo parlamentare o titolare di un mandato.

88. Il funzionario responsabile della distruzione e la persona che ne è testimone firmano un certificato di distruzione, che è depositato e archiviato nell'UIC. L'UIC conserva, insieme ai moduli di distribuzione, i certificati di distruzione relativi alle informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente per un periodo di almeno dieci anni e, nel caso di informazioni classificate di livello «SECRET UE/EU SECRET» o equivalente e di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o equivalente, per un periodo di almeno cinque anni.

89. I documenti che contengono informazioni classificate sono distrutti con metodi conformi alle pertinenti norme dell'Unione o a norme equivalenti in modo da impedire la loro totale o parziale ricostruzione.

90. La distruzione dei supporti informatici delle informazioni classificate avviene conformemente alle pertinenti istruzioni di trattamento.

91. La distruzione delle informazioni classificate è registrata nel repertorio pertinente con i seguenti dati:

a) la data e l'ora della distruzione;

b) il nome del funzionario responsabile della distruzione;

c) l'identificazione del documento o delle copie distrutte;

d) la forma materiale originaria delle ICUE distrutte;

e) i mezzi di distruzione; e

f) il luogo di distruzione;

M. **ARCHIVIAZIONE**

92. Le informazioni classificate, compresi eventuali note/lettere di accompagnamento, allegati, ricevute di deposito e/o altre parti del fascicolo, sono trasferite alla sala di archiviazione protetta sei mesi dopo l'ultima consultazione e al massimo un anno dopo il loro deposito. Norme dettagliate relative all'archiviazione delle informazioni classificate sono stabilite nelle istruzioni sul trattamento.

93. Per «altre informazioni riservate», si applicano le regole generali sulla gestione dei documenti, fatte salve altre disposizioni specifiche sul loro trattamento.

COMUNICAZIONE DI SICUREZZA 3

TRATTAMENTO DELLE INFORMAZIONI RISERVATE MEDIANTE I SISTEMI DI COMUNICAZIONE E INFORMAZIONE (CIS) AUTOMATIZZATI

A. **GARANZIA DI SICUREZZA DELLE INFORMAZIONI CLASSIFICATE TRATTATE NEI SISTEMI DI INFORMAZIONE**

1. Per «garanzia di sicurezza delle informazioni» (IA) nel campo dei sistemi di informazione si intende la fiducia nel fatto che tali sistemi proteggeranno le informazioni classificate che trattano e funzioneranno nel modo dovuto e a tempo debito sotto il controllo degli utenti legittimi. Una IA efficace garantisce gli adeguati livelli di riservatezza, integrità, disponibilità, non disconoscibilità e autenticità. L'IA si basa su una procedura di gestione del rischio.

2. Per «sistema di comunicazione e informazione» (CIS) per il trattamento delle informazioni classificate si intende un sistema che consente il trattamento delle informazioni in forma elettronica. Tale sistema di informazione comprende l'insieme delle risorse necessarie al suo funzionamento, tra cui l'infrastruttura, l'organizzazione, il personale e le risorse dell'informazione.

3. I CIS trattano le informazioni classificate conformemente al concetto di garanzia di sicurezza delle informazioni.

4. I CIS sono sottoposti a una procedura di accreditamento. L'accreditamento ha lo scopo di garantire che siano state messe in atto tutte le misure di sicurezza adeguate e che si sia raggiunto un sufficiente livello di protezione delle informazioni classificate e del CIS, conformemente alla presente comunicazione di sicurezza. La dichiarazione di accreditamento determina il livello di classificazione più elevato delle informazioni che può essere trattato nel CIS nonché i termini e le condizioni ivi associati.

5. Le proprietà e i concetti seguenti in materia di garanzia di sicurezza delle informazioni (IA) sono fondamentali per la sicurezza e il corretto funzionamento operativo dei CIS:

a) autenticità: garanzia che l'informazione è veritiera e proviene da fonti in buona fede;

b) disponibilità: proprietà di accessibilità e utilizzabilità su richiesta di un'entità autorizzata;

c) riservatezza: proprietà per cui l'informazione non deve essere divulgata a persone, enti o procedure non autorizzate;

d) integrità: proprietà di tutela della precisione e della completezza delle informazioni e risorse;

e) non disconoscibilità: capacità di provare che un'azione o un evento siano effettivamente accaduti in modo tale da precludere la possibilità di negare successivamente quell'evento o azione.

B. **PRINCIPI DI GARANZIA DI SICUREZZA DELLE INFORMAZIONI**

6. Le disposizioni esposte di seguito sono alla base della sicurezza di qualsiasi CIS che tratti informazioni classificate. I requisiti d'attuazione dettagliati di queste disposizioni sono definiti nelle politiche e negli orientamenti di sicurezza in materia di IA.

B.1. ***Gestione del rischio di sicurezza***

7. La gestione del rischio di sicurezza è parte integrante della definizione, dello sviluppo, del funzionamento e della manutenzione dei CIS. La gestione del rischio (valutazione, trattamento, accettazione e comunicazione) è condotta congiuntamente, nel quadro di un processo iterativo, da rappresentanti dei proprietari dei sistemi, autorità di progetto, autorità operative e autorità preposte all'approvazione di sicurezza, definiti nella comunicazione di sicurezza 1, avvalendosi di procedure comprovate, trasparenti e comprensibili di valutazione del rischio. La portata del CIS e delle relative risorse è definita in modo chiaro all'inizio della procedura di gestione del rischio.

8. Le autorità competenti, quali definite nella comunicazione di sicurezza 1, esaminano le potenziali minacce ai CIS e tengono costantemente aggiornate e complete le valutazioni dei rischi corrispondenti all'ambiente operativo del momento. Esse si tengono costantemente aggiornate sulle questioni inerenti alla vulnerabilità e rivedono periodicamente la valutazione di vulnerabilità alla luce dell'evoluzione dell'ambiente di tecnologia dell'informazione (TI).

9. Il trattamento del rischio di sicurezza è volto ad applicare una serie di misure di sicurezza che comportino un equilibrio soddisfacente tra le esigenze degli utenti, i costi e il rischio di sicurezza residuo.

10. L'accreditamento di un CIS comprende una dichiarazione formale sul rischio residuo e l'accettazione di tale rischio da parte di un'autorità responsabile. I requisiti, la portata e il grado di dettaglio specifici determinati dalla SAA competente per l'accreditamento di un CIS sono commisurati al rischio valutato, tenendo conto di tutti i fattori pertinenti, tra cui il livello di classificazione delle informazioni classificate trattate nel CIS.

B.2. ***Sicurezza lungo tutto il ciclo di vita del CIS***

11. La garanzia della sicurezza è un obbligo lungo tutto il ciclo di vita del CIS, dall'inizio al ritiro dal servizio.

12. Il ruolo e l'interazione di ciascun attore di un CIS con riferimento alla sua sicurezza è individuato per ciascuna fase del ciclo di vita.

13. Il CIS, comprese le relative misure di sicurezza tecniche e non tecniche, è soggetto a prove di sicurezza durante il processo di accreditamento per garantire un adeguato livello di garanzie di sicurezza e accertare che il CIS, comprese le relative misure di sicurezza tecniche e non tecniche, sia applicato, integrato e configurato correttamente.

14. Le valutazioni, le ispezioni e le verifiche di sicurezza sono effettuate periodicamente durante il funzionamento e la manutenzione del CIS nonché quando si verificano circostanze eccezionali.

15. La documentazione di sicurezza di un CIS evolve durante il suo ciclo di vita come parte integrante del processo di gestione dei cambiamenti.

16. Le procedure di registrazione effettuate dal CIS, ove necessario, sono verificate nel quadro del processo di accreditamento.

B.3. ***Migliori pratiche***

17. L'IAA sviluppa migliori pratiche di protezione delle informazioni classificate trattate dal CIS. Gli orientamenti sulle migliori pratiche stabiliscono misure di sicurezza tecniche, materiali, organizzative e procedurali per i CIS di comprovata efficacia nel combattere determinate minacce e vulnerabilità.

18. La protezione delle informazioni classificate trattate dal CIS si avvale dell'esperienza maturata dalle entità coinvolte nell'IA.

19. La diffusione e successiva attuazione delle migliori pratiche contribuisce al raggiungimento di un livello equivalente di garanzia di sicurezza del CIS gestito dal Segretariato del Parlamento europeo che tratta informazioni classificate.

B.4. ***Difesa in profondità***

20. Al fine di attenuare il rischio per i CIS è attuata una serie di misure di sicurezza tecniche e non tecniche, organizzate come fasi multiple di difesa. Tali fasi comprendono:

a) la deterrenza: misure di sicurezza volte a scoraggiare progetti ostili di attacco dei CIS;

b) la prevenzione: misure di sicurezza volte a ostacolare o bloccare un attacco ai CIS;

c) il rilevamento: misure di sicurezza volte a scoprire un attacco ai CIS;

d) la resilienza: misure di sicurezza volte a limitare l'impatto di un attacco ad una serie minima di informazioni o risorse del CIS evitando ulteriori danni;

e) il ripristino: misure di sicurezza volte a ripristinare il funzionamento in sicurezza del CIS;

Il livello di rigore di tali misure di sicurezza è determinato in base a una valutazione del rischio.

21. Le autorità competenti, come specificato nella comunicazione di sicurezza 1, assicurano di poter rispondere a incidenti che trascendano i limiti organizzativi in modo tale da coordinare le risposte e condividere le informazioni su tali incidenti e i relativi rischi (capacità di risposta in caso di emergenza informatica).

B.5. ***Principio di essenzialità e privilegio minimo***

22. Per evitare rischi inutili sono attuate solo le funzionalità, i dispositivi e i servizi essenziali per soddisfare i requisiti operativi dei sistemi.

23. Agli utenti dei CIS e alle procedure automatizzate sono forniti solo l'accesso, i privilegi o le autorizzazioni necessari allo svolgimento dei loro compiti, limitando così i danni derivanti da incidenti, errori o uso non autorizzato delle risorse dei CIS.

B.6. ***Sensibilizzazione alla garanzia di sicurezza delle informazioni***

24. La sensibilizzazione ai rischi e alle misure di sicurezza disponibili è la prima linea di difesa per la sicurezza dei CIS. In particolare tutto il personale attivo nel ciclo di vita dei CIS, compresi gli utenti, è consapevole di quanto segue:

a) le disfunzioni della sicurezza possono danneggiare gravemente i CIS che trattano le informazioni classificate;

b) il potenziale danno ad altri che può derivare dall'interconnettività e dall'interdipendenza;

c) la responsabilità personale, e l'obbligo di rendere conto, nella sicurezza dei CIS, secondo i rispettivi ruoli all'interno dei sistemi e delle procedure.

25. Per assicurare che le responsabilità in materia di sicurezza siano ben comprese, tutte le persone coinvolte, ivi compresi i quadri dirigenziali, i membri del Parlamento europeo e gli utenti dei CIS, è tenuto a seguire corsi di formazione e sensibilizzazione all'IA.

B.7. ***Valutazione e approvazione dei prodotti di sicurezza TI***

26. I CIS che trattano informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente sono protetti in modo tale che le informazioni non possano essere compromesse da radiazioni elettromagnetiche non intenzionali («misure di sicurezza TEMPEST»).

27. Qualora la protezione delle informazioni classificate sia assicurata mediante prodotti crittografici, questi ultimi sono certificati dalla SAA come prodotti crittografici approvati a livello dell'UE.

28. Per la trasmissione di informazioni classificate con mezzi elettronici si usano prodotti crittografici approvati a livello dell'Unione. In deroga al presente requisito, si possono applicare in situazioni di emergenza procedure o configurazioni tecniche specifiche, come precisato ai punti da 41 a 44.

29. Il livello necessario di fiducia nelle misure di sicurezza, definito quale livello di garanzia, è determinato in base ai risultati della procedura di gestione del rischio e conformemente alle politiche e agli orientamenti pertinenti in materia di sicurezza.

30. Il livello di garanzia è verificato tramite procedure e metodologie riconosciute a livello internazionale o approvate a livello nazionale. Ciò comprende in primo luogo valutazione, controlli e verifiche.

31. La SAA approva orientamenti di sicurezza per la qualificazione e l'approvazione dei prodotti di sicurezza TI non crittografici.

B.8. ***Trasmissione nelle zone protette***

32. Se la trasmissione di informazioni classificate è limitata a zone protette, è possibile procedere a una distribuzione non cifrata o a una cifratura di livello inferiore in base ai risultati di una procedura di gestione del rischio e previa approvazione della SAA.

B.9. ***Sicurezza dell'interconnessione dei CIS***

33. Per interconnessione si intende la connessione diretta tra due o più sistemi TI ai fini della condivisione di dati e di altre risorse dell'informazione in modo unidirezionale o multidirezionale;

34. Il CIS considera inaffidabili i sistemi TI interconnessi e applica misure di protezione per controllare lo scambio di informazioni classificate con qualsiasi altro CIS.

35. Per tutte le interconnessioni dei CIS con un altro sistema TI sono soddisfatti i requisiti di base seguenti:

a) i requisiti commerciali o operativi di tali interconnessioni sono dichiarati e approvati dalle autorità competenti;

b) l'interconnessione in questione è soggetta ad una procedura di gestione del rischio e di accreditamento e richiede l'approvazione della SAA competente;

c) lungo il perimetro del CIS sono attuati servizi di protezione (Protection Services - PS).

36. Non vi è interconnessione tra un CIS accreditato e una rete non protetta o pubblica, ad eccezione dei casi in cui il CIS ha approvato PS installati a tal fine tra il CIS stesso e la rete non protetta o pubblica. Le misure di sicurezza per tali interconnessioni sono esaminate dall'IAA competente e approvate dalla SAA competente.

37. Se la rete non protetta o pubblica è usata solo come vettore e i dati sono criptati con un prodotto crittografico certificato a livello dell'UE conformemente al punto 27, tale connessione non è considerata un'interconnessione.

38. È vietata l'interconnessione diretta o a cascata a una rete non protetta o pubblica di un CIS accreditato per il trattamento di informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente o di livello «SECRET UE/EU SECRET» o equivalente.

B.10. ***Supporti informatici***

39. I supporti informatici sono distrutti secondo procedure approvate dall'autorità di sicurezza competente.

40. I supporti informatici sono riutilizzati, declassati o declassificati secondo le istruzioni relative al trattamento.

B.11. ***Situazioni di emergenza***

41. Le procedure specifiche descritte di seguito possono essere applicate in casi di emergenza, come in situazioni di crisi, conflitti o guerre imminenti o già in corso o in circostanze operative eccezionali.

42. Le informazioni classificate possono essere trasmesse, previo consenso dell'autorità competente, usando prodotti crittografici approvati per un livello di classificazione 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 o non hanno quella necessaria; e

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

43. Le informazioni classificate trasmesse nelle circostanze di cui al punto 41 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 e con altri mezzi del livello di classifica.

44. In caso di ricorso alle disposizioni di cui ai punti 41 o 42, è presentato un successivo rapporto all'autorità competente.

COMUNICAZIONE DI SICUREZZA 4

SICUREZZA MATERIALE

A. **INTRODUZIONE**

La presente nota di sicurezza definisce i principi di sicurezza relativi alla creazione di un ambiente sicuro atto a garantire il corretto trattamento delle informazioni riservate in seno al Parlamento europeo. Tali principi, compresi quelli relativi alla sicurezza tecnica, saranno integrati dalle istruzioni di trattamento.

B. **GESTIONE DEL RISCHIO DI SICUREZZA**

1. Il rischio per le informazioni riservate è gestito secondo un processo volto a determinare i rischi noti per la sicurezza, a definire le misure di sicurezza per contenerli entro un livello accettabile conformemente ai principi fondamentali e alle norme minime contenuti nella presente comunicazione di sicurezza e ad applicare tali misure secondo il concetto di difesa in profondità quale definito nella comunicazione di sicurezza 3. L'efficacia di tali misure è valutata costantemente.

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

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

4. I piani di continuità operativa comprendono misure di prevenzione e recupero per minimizzare l'impatto di disfunzioni o incidenti gravi nel trattamento e nella conservazione delle informazioni riservate.

C. **PRINCIPI GENERALI**

5. Il livello di classificazione o di contrassegno assegnato alle informazioni determina il livello di protezione ad esse attribuito nell'ambito della sicurezza materiale.

6. Le informazioni che danno luogo a classificazione sono contrassegnate e trattate in quanto tali a prescindere dalla loro forma materiale. La classificazione deve essere comunicata in modo chiaro ai destinatari, mediante un contrassegno di classificazione (qualora le informazioni siano comunicate per iscritto, su carta o nell'ambito del CIS) o mediante un annuncio (qualora le informazioni siano comunicate oralmente, per esempio nell'ambito di una conversazione o di una presentazione). Il materiale classificato deve essere contrassegnato fisicamente in modo che la classificazione di sicurezza possa essere facilmente individuata.

7. Le informazioni riservate non devono, in nessun caso, essere lette in luoghi pubblici dove potrebbero essere viste da persone senza la necessità di conoscere, ad esempio sui treni o negli aerei, nei caffé, bar, ecc. Tali informazioni non devono essere lasciate nelle casseforti o nelle camere di alberghi né devono essere lasciate incustodite in luoghi pubblici.

D. **RESPONSABILITÀ**

8. L'UIC ha la responsabilità di assicurare la sicurezza materiale nella gestione delle informazioni riservate depositate nelle sue strutture protette. L'UIC è altresì responsabile della gestione delle sue strutture protette.

9. La responsabilità della sicurezza materiale nella gestione delle informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e delle «altre informazioni riservate» spetta al competente organo parlamentare/titolare di un mandato.

10. La direzione della sicurezza e della valutazione del rischio assicura il nulla osta personale di sicurezza e il nulla osta di sicurezza necessari a garantire il trattamento sicuro delle informazioni riservate all'interno del Parlamento europeo.

11. La DIT fornisce consulenza e provvede a che qualsiasi CIS creato o utilizzato sia pienamente conforme alla comunicazione di sicurezza 3 e alle relative istruzioni di trattamento.

E. **STRUTTURE PROTETTE**

12. Possono essere installate strutture protette a norma delle norme tecniche di sicurezza e in conformità del livello assegnato alle informazioni riservate di cui all'articolo 7.

13. Le strutture protette sono certificate dalla SAA e convalidate dalla SA.

F. **CONSULTAZIONE DELLE INFORMAZIONI RISERVATE**

14. Quando informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e «altre informazioni riservate» sono depositate presso l'UIC e devono essere consultate al di fuori dell'area di sicurezza, l'UIC trasmette una copia al servizio autorizzato competente che garantisce che la consultazione e il trattamento delle informazioni in questione siano conformi all'articolo 8, paragrafo 2, e all'articolo 10 della presente decisione e alle istruzioni di trattamento appropriate.

15. Quando informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e «altre informazioni riservate» sono depositate presso un organo parlamentare/titolare di un mandato diverso dall'UIC, la segreteria di tale organo parlamentare/titolare di un mandato garantisce che la consultazione e il trattamento di tali informazioni siano conformi all'articolo 7, paragrafo 3, all'articolo 8, paragrafi 1, 2 e 4, all'articolo 9, paragrafi 3, 4 e 5, all'articolo 10, paragrafi da 2 a 6 e all'articolo 11 della presente decisione e alle istruzioni di trattamento appropriate.

16. Quando informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente devono essere consultate nella zona protetta, l'UIC garantisce che la consultazione e il trattamento delle informazioni in questione siano conformi agli articoli 9 e 10 della presente decisione e alle istruzioni di trattamento appropriate.

G. **SICUREZZA TECNICA**

17. La responsabilità delle misure di sicurezza tecnica spetta alla SAA, che stabilisce nelle istruzioni di trattamento appropriate le misure specifiche di sicurezza tecnica da applicare.

18. Le sale di lettura protette destinate alla consultazione di informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e di «altre informazioni riservate» rispettano le misure specifiche di sicurezza tecnica come previsto nelle istruzioni di trattamento.

19. La zona protetta comprende le strutture seguenti:

a) una sala adibita al controllo di sicurezza (SAS) da installare conformemente alle misure di sicurezza tecnica di cui alle istruzioni di trattamento. L'accesso a detta struttura avviene mediante registrazione. La SAS osserva norme elevate sotto il profilo dell'identificazione delle persone autorizzate all'accesso, della registrazione video, della zona protetta adibita al deposito degli effetti personali non consentiti nelle sale protette (telefoni, penne, ecc.);

b) una sala comunicazioni adibita alla trasmissione e alla ricezione di informazioni classificate, comprese informazioni classificate criptate, conformemente alla comunicazione di sicurezza 3 e alle relative istruzioni di trattamento;

c) una sala di archiviazione protetta, nella quale sono utilizzati in modo distinto contenitori approvati e certificati per informazioni classificate di livello «RESTREINT UE/EU RESTRICTED», «CONFIDENTIEL UE/EU CONFIDENTIAL» e/o «SECRET EU/EU SECRET», o equivalente. Le informazioni classificate di livello «TRES SECRET UE/EU TOP SECRET» o equivalente sono collocate in una sala distinta in uno specifico contenitore certificato. L'unico materiale aggiuntivo presente in tale sala distinta è la scrivania di supporto per il trattamento dell'archivio da parte dell'UIC;

d) una sala del registro che fornisce gli strumenti necessari per assicurare che la registrazione possa essere fatta in forma cartacea o elettronica e che sia quindi dotata delle necessarie strutture protette per l'installazione del CIS appropriato. Solo la sala del registro può contenere dispositivi di riproduzione approvati e accreditati (per la realizzazione di copie in forma cartacea o elettronica). Le istruzioni di trattamento precisano i dispositivi di riproduzione approvati e accreditati. La sala del registro offre inoltre lo spazio necessario per la conservazione e il trattamento del materiale accreditato consentendo così l'apposizione del contrassegno, la copia e la trasmissione di informazioni classificate in forma materiale in base al livello di classificazione. Tutto il materiale accreditato è definito dall'UIC e accreditato dalla SAA, sulla base del parere ricevuto dall'IAOA. La sala del registro è altresì dotata di un dispositivo di distruzione accreditato e approvato per il livello massimo di classificazione, come descritto nelle istruzioni di trattamento. La traduzione di informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente è effettuata nella sala del registro, nell'apposito sistema accreditato. La sala del registro prevede postazioni di lavoro per un massimo di due traduttori alla volta e per lo stesso documento. Un membro del personale dell'UIC deve essere presente.

e) una sala di lettura, per la consultazione individuale di informazioni classificate da parte di persone debitamente autorizzate. La sala di lettura è dotata di spazio sufficiente per due persone, compreso un membro del personale dell'UIC che deve essere sempre presente durante ogni consultazione. Il livello di sicurezza di questa sala è adeguato per la consultazione di informazioni di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente. La sala di lettura può essere dotata di dispositivi TEMPEST in modo tale da consentire, se del caso, la consultazione elettronica in base al livello di classificazione delle informazioni interessate.

f) una sala riunioni che deve poter accogliere fino a 25 persone ai fini della discussione di informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» o «SECRET EU/EU SECRET», o equivalente. La sala riunioni offre le necessarie strutture tecniche protette e certificate per l'interpretazione da e verso due lingue al massimo. Quando non è utilizzata per riunioni, la sala riunioni può anche essere utilizzata come sala di lettura supplementare per consultazioni individuali. In casi eccezionali, l'UIC può consentire a più di una persona autorizzata di consultare informazioni classificate, purché il grado del nulla osta e la necessità di conoscere sia la stessa per tutte le persone presenti nella sala. Non più di quattro persone sono autorizzate a consultare informazioni classificate allo stesso tempo. La presenza di funzionari dell'UIC deve essere rafforzata.

g) sale tecniche protette per la sistemazione di tutte le apparecchiature tecniche connesse con la sicurezza dell'intera zona protetta e dei server TI protetti.

20. La zona protetta rispetta le norme internazionali applicabili in materia di sicurezza ed è certificata dalla direzione della sicurezza e della valutazione del rischio. La zona protetta contiene le seguenti apparecchiature minime di sicurezza:

a) sistemi di sicurezza di allarme e monitoraggio;

b) dispositivi di sicurezza ed emergenza (sistema di allarme a due vie);

c) un sistema di televisione a circuito chiuso;

d) un sistema di individuazione delle intrusioni;

e) un controllo di accesso (compreso un sistema di sicurezza biometrico);

f) contenitori;

g) armadi;

h) una protezione anti-elettromagnetica.

21. Qualora siano necessarie misure di sicurezza tecniche supplementari, queste possono essere aggiunte dalla SAA, in stretta collaborazione con l'UIC e con l'approvazione della SA.

22. Le apparecchiature dell'infrastruttura possono essere collegate ai sistemi di gestione generali dell'edificio in cui si trova la zona protetta. Tuttavia, i dispositivi di sicurezza dedicati al controllo di accesso e al CIS sono indipendenti da qualsiasi altro sistema del genere esistente all'interno del Parlamento europeo.

H. **ISPEZIONI DELLA ZONA PROTETTA**

23. Le ispezioni della zona protetta sono effettuate periodicamente dalla SAA e su richiesta dell'UIC.

24. La SAA elabora e aggiorna la lista di controllo delle ispezioni di sicurezza per i punti da verificare nel corso di un'ispezione conformemente alle istruzioni di trattamento.

I. **TRASPORTO DELLE INFORMAZIONI RISERVATE**

25. Durante il trasporto le informazioni riservate sono occultate alla vista e non forniscono alcuna indicazione della natura riservata del loro contenuto conformemente alle istruzioni di trattamento.

26. Solo i corrieri o il personale in possesso dell'adeguato livello di autorizzazione di sicurezza possono trasportare informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente.

27. Le informazioni riservate possono essere inviate soltanto tramite posta esterna o trasportate a mano al di fuori di un edificio nel rispetto delle condizioni previste nelle istruzioni di trattamento.

28. Le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET» o equivalente non devono mai essere inviate mediante posta elettronica o fax, anche se tramite un sistema di posta elettronica protetto o un fax criptato. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le altre informazioni riservate possono essere trasmesse per posta elettronica utilizzando un sistema di codifica accreditato.

J. **CONSERVAZIONE DELLE INFORMAZIONI RISERVATE**

29. Il livello di classificazione o di contrassegno assegnato alle informazioni determina il livello di protezione ad esse attribuito ai fini della loro conservazione. Le informazioni sono conservate nel dispositivo certificato a tale scopo conformemente alle istruzioni di trattamento.

30. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate»:

a) sono conservate in un armadio di acciaio chiuso a chiave di dotazione standard in un ufficio o in uno spazio di lavoro quando non sono effettivamente in uso;

b) non devono essere lasciate incustodite a meno che non siano opportunamente conservate sotto chiave;

c) non devono essere lasciate su una scrivania, un tavolo, ecc. in modo tale da poter essere lette o prelevate da persone non autorizzate, ad esempio visitatori, addetti alle pulizie o alla manutenzione, ecc.;

d) non devono essere mostrate o discusse con persone non autorizzate.

31. Le informazioni classificate di livello «RESTREINT UE/EU RESTRICTED» o equivalente e le «altre informazioni riservate» sono conservate esclusivamente presso le segreterie degli organi parlamentari/dei titolari di un mandato o nell'UIC conformemente alle istruzioni di trattamento.

32. Le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL», «SECRET UE/EU SECRET» o «TRÈS SECRET UE/EU TOP SECRET», o equivalente:

a) sono conservate nella zona protetta in un contenitore di sicurezza o in una camera blindata. A titolo eccezionale, ad esempio se l'UIC è chiuso, possono essere conservate in uno scompartimento di sicurezza certificato presso i servizi di sicurezza;

b) non devono mai essere lasciate incustodite nella zona protetta senza essere state precedentemente chiuse a chiave in una cassaforte approvata (anche per assenze brevissime);

c) non devono essere lasciate su una scrivania, un tavolo, ecc. in modo tale da poter essere lette o prelevate da persone non autorizzate, anche se il funzionario responsabile dell'UIC rimane nella stanza.

Qualora un documento contenente informazioni classificate sia prodotto in formato elettronico all'interno della zona protetta, il computer deve essere bloccato e lo schermo deve essere reso inaccessibile se l'originatore o il funzionario responsabile dell'UIC lascia la stanza (anche per assenze brevissime). Un blocco automatico di sicurezza che si attiva dopo alcuni minuti non è considerato una misura sufficiente.

COMUNICAZIONE DI SICUREZZA 5

SICUREZZA INDUSTRIALE

A. **INTRODUZIONE**

1. La presente comunicazione di sicurezza riguarda unicamente le informazioni classificate.

2. Essa stabilisce le disposizioni di applicazione delle norme minime comuni dell'allegato I, parte 1, della presente decisione.

3. Per «sicurezza industriale» si intende l'applicazione di misure che assicurino la protezione di informazioni classificate da parte di contraenti e subcontraenti in sede di negoziati precontrattuali e lungo l'intero il ciclo di vita dei contratti classificati. Tali contratti non contemplano l'accesso alle informazioni classificate di livello «TRÈS SECRET UE/EU TOP SECRET».

4. In quanto autorità contraente, il Parlamento europeo, nell'aggiudicare un contratto classificato a un soggetto industriale o di altra natura, assicura il rispetto delle norme minime sulla sicurezza industriale previste nella presente decisione e a cui fa riferimento il contratto.

B. **ASPETTI DI SICUREZZA DI UN CONTRATTO CLASSIFICATO**

B.1. ***Guida alle classificazioni di sicurezza (SGC)***

5. Prima di indire un bando di gara o di aggiudicare un contratto classificato, il Parlamento europeo, in quanto autorità contraente, determina la classificazione di sicurezza di eventuali informazioni da fornire agli offerenti o contraenti, nonché la classificazione di sicurezza delle eventuali informazioni che il contraente dovrà creare. A tal fine, esso mette a punto una guida alle classificazioni di sicurezza (SGC) in vista dell'esecuzione del contratto.

6. Per stabilire il livello della classificazione di sicurezza dei diversi elementi di un contratto classificato, si applicano i seguenti principi:

a) nel redigere la SGC, il Parlamento europeo tiene conto di tutti gli aspetti di sicurezza del caso, tra cui la classificazione di sicurezza assegnata all'informazione che è fornita e approvata dall'originatore dell'informazione rispetto al contratto.

b) il livello generale di classificazione del contratto non può essere inferiore al livello di classificazione più elevato di uno dei suoi elementi.

B.2. ***Lettera sugli aspetti di sicurezza (SAL)***

7. I requisiti di sicurezza specifici del contratto figurano nella lettera sugli aspetti di sicurezza (SAL). Ove opportuno, tale lettera contiene la guida alle classificazioni di sicurezza ed è parte integrante del contratto o subcontratto classificato.

8. La SAL contiene le disposizioni che impongono al contraente e/o subcontraente di osservare le norme minime figuranti nella presente decisione. L'inosservanza di tali norme minime può costituire motivo di risoluzione del contratto.

B.3. ***Istruzioni di sicurezza del programma/progetto (PSI)***

9. In base alla portata dei programmi o progetti che comportano l'accesso a ICUE, il loro trattamento o la loro conservazione, l'autorità contraente incaricata della gestione del programma o progetto può redigere istruzioni di sicurezza specifiche del programma/progetto interessato.

C. **NULLA OSTA DI SICUREZZA DELLE IMPRESE (FSC)**

10. La NSA o un'altra autorità di sicurezza competente di uno Stato membro rilascia un FSC per indicare, secondo le disposizioni legislative e regolamentari nazionali, che un soggetto industriale o di altra natura è in grado di proteggere le ICUE al livello CONFIDENTIEL UE/ EU CONFIDENTIAL o SECRET UE/EU SECRET, o equivalente all'interno delle proprie strutture. La prova del rilascio del nulla osta è presentata al Parlamento europeo, in quanto autorità contraente, prima che un contraente o subcontraente, effettivo o potenziale, abbia ottenuto accesso alle ICUE.

11. Un FSC è inteso a:

a) valutare l'integrità del soggetto industriale o di altra natura;

b) determinare titolarità, controllo e/o potenziale di influenza indebita che può essere considerato un rischio per la sicurezza;

c) verificare che il soggetto industriale o di altra natura abbia stabilito nella propria struttura un sistema di sicurezza che contempli tutte le opportune misure di sicurezza necessarie ai fini della protezione delle informazioni o del materiale classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET conformemente alle norme minime della presente decisione;

d) verificare che lo status in materia di sicurezza del personale (PSC) (dirigenti, proprietari e dipendenti) che deve avere accesso alle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sia stabilito in modo conforme ai requisiti di cui all'allegato I della presente decisione; e

e) verificare che il soggetto industriale o di altra natura abbia designato un responsabile della sicurezza dell'impresa (FSO), che risponde alla direzione dell'adempimento degli obblighi di sicurezza all'interno del soggetto stesso.

12. Ove opportuno, il Parlamento europeo, in quanto autorità contraente, notifica alla NSA del caso o a un'altra autorità di sicurezza competente l'obbligo di disporre di un FSC in fase precontrattuale o di esecuzione del contratto. In fase precontrattuale è richiesto un FSC o un nulla osta personale di sicurezza (PSC) laddove occorre fornire informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET durante la procedura di presentazione delle offerte.

13. L'autorità contraente non assegna un contratto classificato all'offerente preferenziale finché non ha ricevuto conferma dalla NSA o da un'altra autorità di sicurezza competente dello Stato membro in cui ha sede il contraente o subcontraente interessato che, ove richiesto, è stato rilasciato l'FSC adatto.

14. L'autorità di sicurezza nazionale che ha rilasciato un FSC comunica al Parlamento europeo, in quanto autorità contraente, le eventuali modifiche inerenti all'FSC stesso. Nel caso di un subcontratto, l'autorità di sicurezza competente è informata di conseguenza.

15. La revoca dell'FSC da parte della NSA competente o di un'altra autorità di sicurezza competente è motivo sufficiente perché il Parlamento europeo, in quanto autorità contraente, estingua il contratto classificato o escluda l'offerente dalla gara.

D. **CONTRATTI E SUBCONTRATTI CLASSIFICATI**

16. Qualora a potenziali offerenti siano fornite ICUE in fase precontrattuale, l'invito a presentare offerte contiene una disposizione che impone a un offerente che non ha presentato l'offerta o che non è stato selezionato l'obbligo di restituire tutti i documenti entro un periodo di tempo determinato.

17. Una volta aggiudicato il contratto o il subcontratto classificato, il Parlamento europeo, in quanto autorità contraente, notifica alla NSA del contraente o subcontraente e/o a un'altra autorità di sicurezza competente le disposizioni di sicurezza del contratto classificato.

18. Al momento dell'estinzione di tale contratto, il Parlamento europeo, in quanto autorità contraente (e/o l'autorità di sicurezza competente, a seconda dei casi, se si tratta di un subcontratto), informa senza indugio la NSA o un'altra autorità di sicurezza competente dello Stato membro in cui ha sede il contraente o subcontraente.

19. Di norma, al termine del contratto o subcontratto classificato, il contraente o subcontraente è tenuto a restituire all'ente appaltante le eventuali informazioni classificate in suo possesso.

20. La SAL contiene disposizioni specifiche per l'eliminazione delle informazioni classificate durante l'esecuzione o al termine del contratto.

21. Se è autorizzato a conservare le informazioni classificate alla cessazione del contratto, il contraente o subcontraente continua ad applicare le norme minime comuni previste dalla presente decisione e la riservatezza delle ICUE deve essere protetta dal contraente e dal subcontraente.

22. Le condizioni di subcontrattazione applicabili al contraente sono definite nel bando di gara e nel contratto.

23. Prima di subcontrattare parti di un contratto classificato, il contraente ottiene il consenso del Parlamento europeo in quanto autorità contraente. Nessun subcontratto può essere aggiudicato a un soggetto industriale o di altra natura avente sede in un paese terzo che non abbia concluso un accordo sulla sicurezza delle informazioni con l'Unione.

24. Spetta al contraente garantire che tutte le attività del subcontratto si svolgano secondo le norme minime previste dalla presente decisione; egli non fornisce ICUE al subcontraente senza previo consenso scritto dell'autorità contraente.

25. L'autorità contraente esercita i diritti dell'originatore sulle informazioni classificate create o trattate dal contraente o subcontraente.

E. **VISITE RELATIVE A CONTRATTI CLASSIFICATI**

26. Ove il Parlamento europeo, i contraenti o i subcontraenti richiedano l'accesso a informazioni di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET nei rispettivi locali per l'esecuzione di un contratto classificato, le visite sono fissate di concerto con le NSA o con altre autorità di sicurezza competenti interessate. Tuttavia, nel contesto di progetti specifici, le NSA possono anche concordare una procedura in base alla quale tali visite possono essere fissate direttamente.

27. Tutti i visitatori dispongono di un PSC adatto e della necessità di conoscere per accedere alle informazioni classificate relative a un contratto del Parlamento europeo.

28. I visitatori possono accedere soltanto alle informazioni classificate relative all'oggetto della visita.

F. **TRASMISSIONE E TRASPORTO DI INFORMAZIONI CLASSIFICATE**

29. Per la trasmissione elettronica di informazioni classificate, si applicano le pertinenti disposizioni della comunicazione di sicurezza 3.

30. Per quanto riguarda il trasporto di informazioni classificate, si applicano le pertinenti disposizioni della comunicazione di sicurezza 4 e le istruzioni di trattamento pertinenti.

31. In relazione al trasporto di materiale classificato come carico, in sede di fissazione delle disposizioni di sicurezza si applicano i seguenti principi:

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

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

c) le società addette al trasporto sono dotate di un FSC al livello opportuno; in tal caso, il personale addetto alla spedizione dispone di un nulla osta di sicurezza conformemente all'allegato I;

d) qualsiasi movimento transfrontaliero di materiale classificato di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET, o equivalente è subordinato a un programma di trasporto elaborato dal mittente e approvato dal Segretario generale;

e) i tragitti sono effettuati, per quanto possibile, da un determinato punto di partenza a un determinato punto di arrivo e sono completati quanto più rapidamente possibile;

f) nella misura del possibile, gli itinerari si effettuano attraverso il territorio degli Stati membri.

G. **TRASMISSIONE DI INFORMAZIONI CLASSIFICATE A CONTRAENTI SITUATI IN PAESI TERZI**

32. Le informazioni classificate sono trasmesse a contraenti e subcontraenti situati in paesi terzi secondo le misure di sicurezza convenute tra il Parlamento europeo, in quanto autorità contraente, e il paese terzo interessato in cui il contraente ha sede.

H. **TRATTAMENTO E CONSERVAZIONE DI INFORMAZIONI CLASSIFICATE DI LIVELLO RESTREINT UE/EU RESTRICTED**

33. Di concerto con la NSA dello Stato membro interessato, il Parlamento europeo, in quanto autorità contraente, ha il diritto di procedere a visite dei locali dei contraenti/subcontraenti in forza delle disposizioni contrattuali, per verificare che siano state attuate le misure di sicurezza per la protezione delle ICUE di livello RESTREINT UE/EU RESTRICTED come da contratto.

34. Nella misura in cui è necessario a norma delle disposizioni legislative e regolamentari nazionali, le NSA o altre autorità nazionali competenti sono informate dal Parlamento europeo dei contratti o subcontratti contenenti informazioni classificate di livello RESTREINT UE/EU RESTRICTED.

35. Per i contratti stipulati dal Parlamento europeo contenenti informazioni classificate di livello RESTREINT UE/EU RESTRICTED, i contraenti o subcontraenti e il relativo personale non sono tenuti a possedere un FSC o un PSC.

36. Il Parlamento europeo, in quanto autorità contraente, esamina le risposte agli inviti a presentare offerte per i contratti che richiedono l'accesso a informazioni classificate di livello RESTREINT UE/EU RESTRICTED, a prescindere da eventuali requisiti vigenti a norma delle disposizioni legislative e regolamentari nazionali in ordine agli FSC o PSC.

37. Le condizioni di subcontrattazione applicabili al contraente sono definite nel bando di gara e nel contratto.

38. Se un contratto comporta il trattamento di informazioni classificate di livello RESTREINT UE/EU RESTRICTED nei sistemi di comunicazione e informazione gestiti da un contraente, il Parlamento europeo, in quanto autorità contraente, garantisce che nel contratto o eventuale subcontratto siano specificati i requisiti tecnici e amministrativi necessari in ordine all'accreditamento dei sistemi di comunicazione e informazione commisurati al rischio valutato, tenendo conto di tutti i fattori pertinenti. La portata dell'accreditamento di tali sistemi di comunicazione e informazione è concordata tra l'autorità contraente e la NSA competente.

COMUNICAZIONE DI SICUREZZA 6

VIOLAZIONI DELLA SICUREZZA, PERDITA O COMPROMISSIONE DI INFORMAZIONI RISERVATE

1. La violazione della sicurezza è conseguenza di atti o omissioni contrari alla presente decisione che potrebbero mettere a repentaglio o compromettere informazioni riservate.

2. Le informazioni riservate sono compromesse quando esse, o parte di esse, giungono in possesso di persone non autorizzate, ad esempio persone che siano sprovviste dell'apposito nulla osta di sicurezza o che non abbiano la necessaria esigenza di conoscerle, o qualora esista la probabilità che si sia verificata tale circostanza.

3. Le informazioni riservate possono essere compromesse per disattenzione o negligenza, a seguito di indiscrezioni o come conseguenza delle attività di servizi che prendono di mira l'Unione o di organizzazioni sovversive.

4. Qualora il Segretario generale riscontri o sia informato di una violazione della sicurezza, della perdita o della compromissione, comprovate o sospette, di informazioni riservate, egli:

a) accerta i fatti;

b) valuta e limita per quanto possibile i danni;

c) adotta misure volte a impedire che i fatti si ripetano;

d) informa l'autorità competente della parte terza o dello Stato membro da cui provengono le informazioni riservate o che le ha trasmesse.

Qualora sia coinvolto un deputato al Parlamento europeo, il Segretario generale agisce d'intesa con il Presidente del Parlamento.

Se le informazioni sono ottenute da un'altra istituzione dell'Unione, il Segretario generale agisce secondo le opportune misure di sicurezza relative alle informazioni classificate e le disposizioni vigenti stabilite in conformità dell'accordo quadro con la Commissione o dell'accordo interistituzionale con il Consiglio.

5. Tutte le persone che trattano informazioni riservate ricevono informazioni dettagliate riguardo alle procedure di sicurezza, ai pericoli derivanti da conversazioni indiscrete e alle proprie relazioni con i mezzi di comunicazione e, se del caso, firmano una dichiarazione con cui si impegnano a non divulgare informazioni riservate a terzi, a rispettare l'obbligo di proteggere le informazioni classificate e a prendere atto delle conseguenze dell'eventuale inosservanza delle presenti disposizioni. L'accesso alle informazioni classificate o il loro utilizzo da parte di una persona che non abbia ricevuto le opportune informazioni e non abbia firmato la relativa dichiarazione è da considerarsi una violazione della sicurezza.

6. I deputati al Parlamento europeo, i funzionari del Parlamento e gli altri agenti del Parlamento impiegati presso i gruppi politici o i contraenti riferiscono immediatamente al Segretario generale qualsiasi violazione della sicurezza, perdita o compromissione di informazioni riservate di cui vengano a conoscenza.

7. Il responsabile della compromissione di informazioni riservate è passibile di sanzioni disciplinari secondo le disposizioni normative e regolamentari pertinenti. Tali sanzioni non pregiudicano eventuali azioni legali che potrebbero essere avviate conformemente alla legge applicabile.

8. Fatte salve ulteriori azioni legali, le violazioni commesse da funzionari del Parlamento e altri agenti del Parlamento impiegati presso i gruppi politici comportano l'applicazione delle procedure e delle sanzioni previste dal titolo VI dello statuto dei funzionari.

9. Fatte salve ulteriori azioni legali, le violazioni commesse da deputati al Parlamento europeo sono trattate conformemente all'articolo 9, paragrafo 2, e agli articoli 152, 153 e 154 del regolamento del Parlamento europeo.