IV

(Informazioni)

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

PARLAMENTO EUROPEO

DECISIONE DELL'UFFICIO DI PRESIDENZA DEL PARLAMENTO EUROPEO

del 6 giugno 2011

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

(2011/C 190/02)

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»), é necessario rivedere la decisione dell'Ufficio di presidenza del 13 novembre 2006 sulla regolamentazione relativa al trattamento amministrativo dei documenti riservati.

(2) Il trattato di Lisbona attribuisce nuovi compiti al Parlamento europeo e che, 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 impregiudicati l'articolo 15 del trattato sul funzionamento dell'Unione europea (TFUE) e il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione [2].

(5) Le disposizioni della presente decisione lasciano impregiudicati l'articolo 16 TFUE e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [3],

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Obiettivo

La presente decisione disciplina la creazione, la ricezione, la trasmissione e la conservazione di informazioni riservate da parte del Parlamento europeo ai fini di un'adeguata tutela della loro natura riservata. Essa attua, in particolare, l'allegato 2 dell'accordo quadro.

[1] GU L 304 del 20.11.2010, pag. 47.

[2] GU L 145 del 31.5.2001, pag. 43.

[3] GU L 8 del 12.1.2001, pag. 1.

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 UE» (ICUE) e «altre informazioni riservate» non classificate;

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

— «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo): é la classificazione per 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): é la classificazione per 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): é la classificazione per 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): é la classificazione per le informazioni e i materiali la cui divulgazione non autorizzata potrebbe pregiudicare gli interessi dell'Unione o di uno o più Stati membri;

d) «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 o trasmesse a quest'ultimo da altre istituzioni, organismi, agenzie istituite in virtù o sulla base dei trattati o da Stati membri;

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

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

g) «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;

h) «autorizzazione» indica una decisione (decisione di nulla osta) adottata dal presidente se riguarda deputati al Parlamento europeo e del segretario generale se riguarda funzionari del Parlamento europeo e altri agenti del Parlamento impiegati presso i gruppi politici, con la quale si concede l'accesso individuale alle ICUE 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;

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

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

k) «originatore» indica l'autore debitamente autorizzato di ICUE o di qualsiasi altra informazione riservata;

l) «comunicazioni di sicurezza» indica misure tecniche di attuazione di cui all'allegato II [1].

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 i principi fondamentali e le norme minime, il quale 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;

Nel quale il trattamento delle informazioni riservate mediante i sistemi informativi (IS) automatizzati del Parlamento europeo ha luogo secondo il concetto di garanzia di sicurezza delle informazioni (IA) ed è stabilito nelle comunicazioni di sicurezza.

[1] Allegato da adottare.

3. I deputati al Parlamento europeo possono consultare le informazioni classificate fino al livello CONFIDENTIEL UE/EU CONFIDENTIAL compreso senza nulla osta di sicurezza. Per quanto riguarda le informazioni classificate come CONFIDENTIEL UE/EU CONFIDENTIAL, essi sottoscrivono una dichiarazione solenne di non rivelarne il contenuto a terzi. Le informazioni classificate di livello superiore a CONFIDENTIEL UE/EU CONFIDENTIAL sono unicamente messe a disposizione dei deputati muniti dell'adeguato livello di nulla osta di sicurezza.

4. 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 classificate di livello superiore a RESTREINT UE/EU RESTRICTED se sono muniti dell'adeguato livello di nulla osta di sicurezza.

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 al Servizio per le informazioni riservate (SIR) quando il documento è depositato presso di esso.

3. Le informazioni riservate coperte da segreto professionale sono trattate conformemente alle istruzioni contenute nelle comunicazioni di sicurezza.

Articolo 5

Ricezione di informazioni riservate da parte del Parlamento europeo

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

— ICUE qualificate di livello RESTREINT UE/EU RESTRICTED (UE riservato) e altre informazioni riservate alla segreteria dell'organo parlamentare/del titolare di un mandato che ne ha fatto richiesta,

— ICUE qualificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL (UE Riservatissimo) e superiore, al SIR.

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

3. In caso di informazioni riservate comunicate dalla Commissione sulla base dell'accordo quadro, le disposizioni concordate ai sensi dell'allegato II, punto 3.2 dell'accordo quadro (stabilito di «comune accordo» e relativo ai destinatari, alla procedura di consultazione, ossia sala di lettura sicura, riunione a porte chiuse, o altre), concepite per garantire la riservatezza delle informazioni, sono depositate insieme alle informazioni riservate presso la segreteria dell'organo parlamentare/del titolare di un mandato o presso il SIR quando le informazioni sono qualificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore.

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. La trasmissione al Parlamento europeo di ICUE classificate di livello TRÈS SECRET UE/EU TOP SECRET è soggetta a ulteriori regole, da concordarsi tra l'organo parlamentare/il titolare di un mandato che ne ha fatto richiesta e le istituzioni UE o gli Stati membri che le trasmettono. La conferenza dei presidenti istituisce una commissione di controllo, il cui scopo è garantire un livello di protezione commisurato a tale livello di classificazione.

Articolo 6

Comunicazione delle ICUE da parte del Parlamento europeo a terzi

Il Parlamento europeo può, previo consenso dell'originatore, trasmettere ICUE ad altre istituzioni, organi e organismi istituiti in virtù dei trattati o agli Stati membri, 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

Conservazione e consultazione di informazioni riservate in zone protette (sale di lettura protette)

1. Una sala di lettura protetta consente la conservazione delle informazioni in sicurezza e non contiene fotocopiatrici, telefoni, fax, scanner o altri mezzi tecnici di riproduzione o trasmissione di documenti.

2. Si applicano le seguenti condizioni di accesso alla sala di lettura protetta:

a) vi hanno accesso unicamente le seguenti persone:

— i deputati al Parlamento europeo, i funzionari del Parlamento europeo e gli altri agenti del Parlamento impiegati presso i gruppi politici debitamente identificati, secondo il disposto dell'articolo 4, paragrafo 2, o dell'articolo 5, paragrafi 3 e 4,

— i funzionari del Parlamento europeo responsabili della gestione del SIR,

— se necessario, i funzionari del Parlamento europeo responsabili della sicurezza e della protezione antincendio.

La pulizia della zona protetta avviene solo in presenza e sotto stretta sorveglianza di un funzionario in forza presso il SIR;

b) ogni persona che intenda consultare le informazioni riservate comunica in anticipo il proprio nominativo al SIR. Quest'ultimo controlla l'identità di ciascuna persona che presenta una richiesta in tal senso, verificando eventualmente se è munita del livello necessario di nulla osta di sicurezza e se è autorizzata alla consultazione, in base al disposto dell'articolo 4, paragrafo 2, o dell'articolo 5, paragrafi 3 e 4;

c) il SIR ha la facoltà di rifiutare l'accesso alla sala a chiunque non sia autorizzato in virtù delle precedenti lettere a) e b). Qualsiasi contestazione della decisione del SIR è sottoposta al presidente qualora si tratti di deputati al Parlamento europeo, e al segretario generale negli altri casi.

3. Le seguenti disposizioni disciplinano la consultazione delle informazioni riservate nella sala di lettura protetta:

a) le persone autorizzate a consultare informazioni e che hanno presentato la domanda di cui al paragrafo 2, lettera b), si presentano di persona presso il SIR.

Salvo circostanze eccezionali (ad esempio, un elevato numero di richieste di consultazione in un breve lasso di tempo), solo una sola persona alla volta è autorizzata a consultare le informazioni riservate nella sala di lettura protetta, alla presenza di un funzionario del SIR.

Detto funzionario comunica alla persona autorizzata i suoi obblighi e, in particolare, le fa firmare una dichiarazione solenne che la impegna a non divulgare le informazioni alle quali ha avuto accesso;

b) durante la lettura non sono autorizzati contatti con l'esterno (compreso mediante l'uso del telefono o di altre tecnologie), annotazioni né la riproduzione mediante fotocopia o fotografia delle informazioni riservate consultate;

c) prima di autorizzare una persona a lasciare la sala di lettura sicura, il funzionario del SIR di cui alla lettera a) si assicura che le informazioni riservate consultate siano ancora presenti, integre e complete.

4. In caso di infrazione alle norme di cui sopra, il responsabile del SIR è tenuto a informarne il segretario generale, che ne riferisce al presidente qualora il responsabile delle infrazioni sia un deputato al Parlamento europeo.

Articolo 8

Norme minime applicabili ad altri tipi di consultazione di informazioni riservate

1. Per quanto riguarda il trattamento amministrativo delle informazioni riservate durante una riunione a porte chiuse, la segreteria dell'organo parlamentare/del titolare di un mandato responsabile per la riunione assicura che:

— solo le persone designate a partecipare alla riunione e titolari del necessario livello di nulla osta di sicurezza siano autorizzate a entrare nella sala riunioni,

— i documenti siano numerati, distribuiti all'inizio della riunione e raccolti al termine della stessa, che non si prendano note del loro contenuto o che non siano eseguite fotocopie o fotografie,

— il verbale della riunione non faccia alcun riferimento al contenuto della discussione dell'informazione trattata secondo la procedura riservata,

— le informazioni riservate trasmesse oralmente a destinatari in seno al Parlamento europeo siano soggette a un livello di protezione equivalente a quello applicato alle informazioni riservate trasmesse per iscritto. Ciò può includere una dichiarazione ufficiale da parte dei destinatari dell'informazione che li impegna a non divulgarne il contenuto a terzi.

2. Per quanto riguarda il trattamento amministrativo delle informazioni riservate da parte della segreteria dell'organo parlamentare/del titolare di un mandato al di fuori della riunione a porte chiuse si applicano le disposizioni seguenti:

— i documenti in formato cartaceo sono consegnati di persona al capo della segreteria, che li registra ed emette un avviso di ricevimento,

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

— fatto salvo il trattamento amministrativo delle informazioni riservate durante una riunione a porte chiuse di cui al paragrafo 1, esse non possono essere in nessun caso duplicate, salvate su un altro supporto, o trasmesse ad altre persone,

— l'accesso a tali documenti è limitato ai destinatari e avviene sotto la supervisione della segreteria, in conformità con le disposizioni di cui all'articolo 4, paragrafo 2, all'articolo 5, paragrafo 3 o all'articolo 5, paragrafo 4,

— la segreteria tiene un registro delle persone che hanno consultato i documenti unitamente alla data e all'ora di tale consultazione. Tale registro é trasmesso al SIR nel quadro della relazione annuale di cui all'articolo 12.

Articolo 9

Archiviazione dei documenti riservati

1. Nei locali del Parlamento europeo è assicurato un sistema protetto di archiviazione.

Le informazioni riservate depositate in via definitiva presso il SIR o presso il segreteria dell'organo parlamentare/il titolare di un mandato sono trasferite alla sala di archiviazione protetta sei mesi dopo l'ultima consultazione e al massimo un anno dopo il loro deposito.

2. Il SIR è responsabile della gestione degli archivi protetti, conformemente a criteri standard di archiviazione.

3. Le informazioni riservate conservate presso gli archivi riservati possono essere consultate alle seguenti condizioni:

— sono autorizzate unicamente le persone identificate per nome o per la loro funzione tramite il documento di accompagnamento stilato al momento del deposito dell'informazione riservata,

— la domanda di consultazione deve essere presentata al SIR, che trasferisce il documento in questione alla sala di lettura protetta,

— si applicano le procedure e le condizioni che disciplinano la consultazione delle informazioni riservate di cui all'articolo 7.

Articolo 10

Declassamento e declassificazione delle ICUE

1. Le ICUE possono essere declassate o declassificate unicamente con il consenso dell'originatore e, se necessario, previa discussione con altre parti interessate. 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.

2. La declassificazione di documenti conservati negli archivi riservati ha luogo al più tardi dopo 30 anni ai sensi delle disposizioni del regolamento (CEE, Euratom) n. 354/83 del Consiglio, del 1º febbraio 1983, che rende accessibili al pubblico gli archivi storici della Comunità economica europea e della Comunità europea dell'energia atomica [1]. La declassificazione è effettuata dall'originatore dell'informazione classificata o dal servizio responsabile a norma dell'allegato I, parte 1, sezione 10.

Articolo 11

Violazioni della riservatezza

1. Le violazioni della riservatezza in generale e della presente decisione in particolare comportano, qualora si tratti di deputati al Parlamento europeo, l'applicazione delle pertinenti disposizioni in materia di sanzioni di cui al regolamento del Parlamento europeo.

2. Le violazioni commesse da membri del personale comportano 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 [2] («Statuto dei funzionari»).

3. Il presidente e il segretario generale organizzano tutte le indagini necessarie.

Articolo 12

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 presenta una relazione annuale all'Ufficio di presidenza sull'applicazione della presente decisione.

[1] GU L 43 del 15.2.1983, pag. 1.
[2] GU L 56 del 4.3.1968, pag. 1.

Articolo 13

Disposizioni transitorie e finali

1. Le informazioni riservate esistenti presso il SIR o negli archivi prima dell'applicazione della presente decisione sono automaticamente classificate di livello RESTREINT UE/EU RESTRICTED, a meno che l'autore decida di non classificarle o di classificarle a un livello di sicurezza superiore o apponendovi un contrassegno entro un anno dalla data di entrata in vigore della presente decisione.

2. Se l'originatore decide di attribuire a tali informazioni confidenziali un livello di classificazione superiore, esse sono classificate al livello più basso possibile dall'originatore o dai suoi delegati, d'intesa con il SIR e conformemente ai criteri di cui all'allegato I.

3. La decisione dell'Ufficio di presidenza del 13 novembre 2006 sulla regolamentazione relativa al trattamento amministrativo dei documenti riservati è abrogata.

4. La decisione dell'Ufficio di presidenza del 24 ottobre 2005, con la quale il segretario generale è incaricato di istituire un comitato di declassificazione e di adottare decisioni in materia di declassificazione, è abrogata.

Articolo 14

Entrata in vigore

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

2. Essa si applica a partire dal 1º luglio 2011.

ALLEGATO I

PARTE 1

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

1. Introduzione

Con le presenti disposizioni si stabiliscono i principi fondamentali e le norme minime di sicurezza che devono essere osservate dal Parlamento europeo in tutte le sue sedi di servizio e da tutti i destinatari di ICUE 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. Esse sono corredate da norme 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.

Il principio della 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. Questo concetto implica altresì che le responsabilità nel campo della sicurezza debbano 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. Un'altra implicazione, infine, è che le violazioni della sicurezza nell'ambito di responsabilità del Parlamento europeo devono essere affrontate in maniera coerente con la politica del Parlamento europeo in materia disciplinare.

Il principio della 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. Esso presuppone altresì l'esistenza di chiari orientamenti scritti per l'attuazione delle misure di sicurezza.

Il principio della 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.

Il principio di 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. Inoltre, in base al principio di sussidiarietà gli interventi nel campo della sicurezza devono essere limitati a quanto é assolutamente necessario e le misure di sicurezza devono essere proporzionate agli interessi da tutelare e alle minacce, reali o potenziali, contro tali interessi, in modo che essi possano essere difesi con il minor danno possibile.

3. Fondamenti della sicurezza dell'informazione

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

a) all'interno del Parlamento europeo, un'autorità INFOSEC — servizio di garanzia della sicurezza dell'informazione — incaricata di collaborare con l'autorità di sicurezza competente per fornire informazioni e consulenza circa le minacce tecniche alla sicurezza e i relativi mezzi di protezione;

b) una stretta collaborazione tra i servizi responsabili del Parlamento europeo e i servizi di sicurezza delle altre istituzioni UE.

4. Principi di sicurezza delle informazioni

4.1. *Obiettivi*

La sicurezza delle informazioni persegue principalmente i seguenti obiettivi:

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

b) proteggere le ICUE 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 ICUE dal sabotaggio e dal danneggiamento intenzionale premeditato;

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

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 particolarmente importante 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 va adottato nella pianificazione e nell'organizzazione della lotta contro lo spionaggio, il sabotaggio, il terrorismo e altre minacce, in modo da garantire la massima protezione ai principali edifici in cui sono collocate ICUE e ai punti più sensibili all'interno di questi.

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

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

4.2.5. Se più elementi d'informazione sono uniti congiuntamente, il grado di classificazione da conferire all'insieme deve essere almeno equivalente a quello dell'elemento con grado di classificazione più elevato applicato individualmente a tali elementi. A una raccolta di informazioni può essere tuttavia conferito un grado di classificazione più elevato di quello dei suoi elementi costitutivi.

4.2.6. Le classificazioni sono assegnate 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 ICUE, ai supporti contenenti ICUE e alle altre informazioni riservate, nonché a tutti i locali che contengono tali informazioni e a importanti installazioni;

b) sono destinate a individuare le persone che, per la loro situazione, 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 ICUE, all'interno dell'istituzione e nei servizi soggetti alla sua competenza, compresi i 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 a tali informazioni a organismi esterni solo a condizione che essi garantiscano che, nel trattarle, siano rispettate disposizioni 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 ICUE 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 certificare 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 si stabilisce che rappresenta un pericolo per la sicurezza, detto individuo deve essere allontanato o rimosso 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 ICUE.

7.1. *Necessità di protezione*

Il grado di sicurezza materiale da applicare per garantire la protezione delle ICUE deve essere proporzionato alla classificazione, al volume e alle minacce che incombono sulle informazioni e sul materiale custodito. Tutti i detentori di ICUE 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 ICUE senza sorveglianza, le persone che ne hanno la custodia devono assicurarsi 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 ICUE o sistemi di comunicazione e d'informazione protetti devono essere tutelati contro l'accesso non autorizzato.

Il tipo di protezione destinato alle ICUE, 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;

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 la protezione delle informazioni classificate durante un'emergenza.

8. **Indicazioni di sicurezza, contrassegni, apposizioni e gestione della classificazione**

8.1. *Indicazioni di sicurezza*

Non è consentita classificazione diversa da quella definita all'articolo 2 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). Tali indicazioni possono essere: «FINO A … (termine/data)» o «FINO A … (evento)».

Qualora risultino necessari una distribuzione limitata e un trattamento speciale oltre a quanto indicato dalla classificazione di sicurezza, si appongono indicazioni supplementari quali CRYPTO o qualunque altra indicazione di sicurezza riconosciuta a livello UE.

Le indicazioni di sicurezza possono essere utilizzate soltanto unitamente a una classificazione.

8.2. *Contrassegni*

Un contrassegno può essere usato per specificare un settore che forma oggetto del documento o una distribuzione particolare sulla base del principio della necessità di sapere, ovvero per indicare il termine di un embargo (nel caso di informazioni non classificate).

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

8.3. *Apposizione della classificazione*

La classificazione si appone nel modo seguente:

a) su documenti classificati di livello «RESTREINT UE/EU RESTRICTED» (UE riservato) con mezzi meccanici o elettronici;

b) su documenti classificati di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» (UE riservatissimo) con mezzi meccanici o a mano o a stampa su carta prestampigliata e registrata;

c) su documenti classificati di livello «SECRET UE/EU SECRET» (UE segreto) e «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo) con mezzi meccanici e a mano.

Le indicazioni di sicurezza sono apposte immediatamente sotto la classificazione, con lo stesso mezzo usato per la classificazione.

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 emanare documenti «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo) è limitato al minimo e il loro nominativo figura in un elenco compilato dal SIR.

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 c). È importante che la classificazione sia attribuita correttamente e con moderazione, in particolare per quanto riguarda la classificazione di livello «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo).

Il grado di classificazione attribuito a una lettera o nota cui è accluso altro materiale corrisponde 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 tiene presenti le disposizioni sopraelencate e limita la tendenza alla 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 del Parlamento europeo compie ispezioni periodiche della normativa di sicurezza per la protezione delle ICUE; essa può essere assistita in tale compito dal SIR.

La direzione della sicurezza e la valutazione del rischio del Parlamento e i servizi della sicurezza di altre istituzioni, organi e organismi istituiti in virtù o sulla base dei trattati o dagli Stati membri che detengono ICUE possono inoltre decidere di comune accordo di effettuare valutazioni tra pari delle normative di sicurezza per la protezione delle ICUE.

10. **Procedura di declassificazione**

10.1. Il SIR esamina le ICUE e avanza proposte sulla declassificazione all'originatore di un documento entro il 25º anno successivo alla data della sua creazione. I documenti non declassificati a seguito di un primo esame sono riesaminati periodicamente e comunque almeno ogni cinque anni.

10.2. Oltre ai documenti conservati negli archivi sicuri e debitamente classificati, la procedura di declassificazione può coprire anche altre informazioni riservate presenti negli archivi sicuri o presso il centro archivistico e documentale del Parlamento europeo (CARDOC).

10.3. Il SIR è tenuto a informare, per conto dell'originatore, i destinatari del documento 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.

10.4. La declassificazione lascia impregiudicati eventuali contrassegni che possano figurare sul documento.

10.5. 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 del SIR.

10.6. Il testo del documento declassificato 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 (CEE, Euratom) n. 354/83 del Consiglio.

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, il SIR consulta il terzo interessato prima di procedere alla declassificazione. Il terzo dispone di un periodo di otto settimane per presentare osservazioni;

b) per quanto concerne eccezioni relative alla vita privata e all'integrità dell'individuo, la procedura di declassificazione tiene conto in particolare del consenso della persona interessata, dell'impossibilità di identificare la persona interessata e/o del fatto che tale persona non sia più in vita;

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. Tenuto conto delle prerogative e delle competenze del Parlamento europeo, ai suoi deputati può essere accordato l'accesso alle ICUE sino al livello «CONFIDENTIEL UE/EU CONFIDENTIEL» (UE riservatissimo) compreso, senza nulla osta di sicurezza. Per le informazioni classificate di livello «CONFIDENTIEL UE/EU CONFIDENTIAL» essi firmano una dichiarazione solenne in cui si impegnano a non diffondere tali informazioni a terzi.

11.2. Per poter accedere alle informazioni classificate di livello «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo) o «SECRET UE/EU SECRET» (UE segreto), i deputati al Parlamento europeo devono essere stati autorizzati a tal fine secondo la procedura di cui ai punti 11.3 e 11.4.

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 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 responsabile per la sicurezza 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 11.15.

11.6. 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. Esso può essere rinnovato secondo la procedura di cui al punto 11.4.

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 le autorità nazionali competenti dello Stato membro esprimono parere positivo, il presidente può rilasciare l'autorizzazione al deputato al Parlamento europeo interessato.

11.13. Se le autorità nazionali competenti esprimono 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 alle autorità nazionali competenti per chiarimenti complementari. In caso di riconferma del parere negativo, l'autorizzazione non può essere rilasciata.

11.14. Ogni deputato al Parlamento europeo che abbia ottenuto l'autorizzazione a norma del punto 11.3 riceve, 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 delle autorità nazionali competenti 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 classificate di livello «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo).

12. **Procedura per il rilascio del nulla osta di sicurezza ai funzionari del Parlamento europeo e altri agenti impiegati presso i gruppi politici**

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 classificate di livello «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo), «SECRET UE/EU SECRET» (UE segreto) e «CONFIDENTIEL UE/EU CONFIDENTIAL» (UE riservatissimo), le persone di cui punto 12.1 devono essere state autorizzate 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 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 responsabile per la sicurezza 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, che 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 interessati, 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 della persona interessata 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 classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore.

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 alle autorità nazionali competenti il segretario generale specifica il tipo e il grado di classificazione delle informazioni di cui la persona interessata dovrà prendere visione, per consentire loro di svolgere l'indagine di sicurezza ed esprimere un parere per il grado di abilitazione appropriato da rilasciare alla persona in questione.

12.11. Per lo svolgimento e i risultati della procedura relativa all'indagine di sicurezza condotta 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.

12.12. Se le autorità nazionali competenti degli Stati membri esprimono parere positivo, il segretario generale può rilasciare l'autorizzazione alla persona interessata.

12.13. Se le autorità nazionali competenti esprimono parere negativo, il funzionario del Parlamento europeo o altro agente del Parlamento impiegato presso i gruppi politici interessati è informato di tale parere e può chiedere di essere ascoltato dal segretario generale. Il segretario generale può, se lo ritiene necessario, rivolgersi alle autorità nazionali competenti 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. Detto 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 delle autorità nazionali competenti e in mancanza di reazioni da parte di queste ultime 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 classificate di livello «TRÈS SECRET UE/EU TOP SECRET» (UE segretissimo).