CORTE
DEI CONTI
EUROPEA

Decisione n. 041-2021 della Corte dei conti sulle norme di sicurezza per proteggere le informazioni classificate UE (ICUE)

LA CORTE DEI CONTI EUROPEA,

VISTO l'articolo 13 del trattato sull'Unione europea,

VISTO l'articolo 287 del trattato sul funzionamento dell'Unione europea (TFUE),

VISTO l'articolo 257 del regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione,

VISTO l'articolo 1, paragrafo 6, della decisione n. 21-2021 della Corte dei conti recante modalità di applicazione del regolamento interno della Corte dei conti,

VISTE le norme di sicurezza per proteggere le informazioni classificate UE della altre istituzioni, agenzie e organismi dell'UE,

VISTE le politiche della Corte dei conti in materia di sicurezza delle informazioni (DEC 127/15 FINAL) e di classificazione delle informazioni (COMPERS 123/2020),

CONSIDERATO CHE ai sensi dell'articolo 287, paragrafo 3, del TFUE, la Corte dei conti ha il diritto di accedere a tutti i documenti e informazioni, comprese le informazioni classificate UE (ICUE), pertinenti e necessari, a suo giudizio, all'espletamento del suo mandato, che va eseguito nel pieno rispetto del principio di leale cooperazione tra le istituzioni e del principio delle attribuzioni conferite; il diritto di accesso alle ICUE, garantito dal TFUE, non può essere rimesso in discussione dal loro originatore, sebbene alla Corte dei conti possa essere chiesto di porre in essere e rispettare determinate misure di sicurezza, come di seguito specificato;

CONSIDERATO CHE i Membri della Corte dei conti, nonché i suoi funzionari e altri agenti, sono tenuti, anche dopo la cessazione dal servizio, all'obbligo di riservatezza di cui all'articolo 339 del TFUE e all'articolo 17 dello statuto del personale, nonché agli atti adottati in applicazione degli stessi;

CONSIDERATO CHE data la loro natura sensibile, il trattamento delle ICUE comporta che il rispetto dell'obbligo di riservatezza si assicurato mediante adeguate misure di sicurezza in grado di garantire un livello elevato di protezione per tali informazioni e che siano equivalenti a quelle stabilite dalla norma sulla protezione delle ICUE adottate da altre istituzioni, agenzie e organismi dell'UE, inteso che la Corte dei conti, qualora considera una siffatta misura di sicurezza ingiustificata alla luce della natura e del tipo di ICUE, si riserva il diritto di

formulare le osservazioni che riterrà opportune, seppur in osservanza del livello di classifica delle ICUE;

CONSIDERATO CHE le misure di sicurezza per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni comunicate alla Corte dei conti devono essere adeguate alla natura e al tipo di informazioni in causa;

CONSIDERATO CHE l'accesso a informazioni classificate deve essere consentito alla Corte dei conti conformemente al principio della necessità di sapere allo scopo di espletare i compiti che le sono stati assegnati dai trattati e dagli atti giuridici adottati sulla loro base;

CONSIDERATO CHE data la natura e il contenuto sensibile di talune informazioni, è opportuno stabilire una procedura speciale per il trattamento da parte della Corte dei conti di documenti contenenti ICUE;

CONSIDERATO CHE l'istituzione deve far sì che la presente decisione sia attuata nel rispetto di tutte le norme applicabili, in particolare delle disposizioni sulla protezione dei dati personali, sulla sicurezza materiale delle persone, degli edifici e delle risorse informatiche, nonché sull'accesso pubblico ai documenti;

DECIDE:

Articolo 1. Oggetto e ambito di applicazione

1) La presente decisione stabilisce i princìpi fondamentali e le norme minime di sicurezza per la protezione delle informazioni classificate trattate dalla Corte dei conti nell'esercizio del suo mandato.

2) Ai fini della presente decisione, per informazioni classificate si intendono uno o tutti i seguenti tipi di informazioni:

   a) "informazioni classificate UE" (ICUE) quali definite nelle norme di sicurezza di altre istituzioni, agenzie, organi o uffici dell'UE e recanti uno dei seguenti contrassegni di classifica di sicurezza:

      - TRÈS SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
      - SECRET UE/EU SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
      - CONFIDENTIEL UE/EU CONFIDENTIAL informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
      - RESTREINT UE/EU RESTRICTED: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri.

b) informazioni classificate fornite dagli Stati membri e recanti un contrassegno di classifica di sicurezza nazionale equivalente a uno dei contrassegni di classifica di sicurezza delle ICUE[1] elencati alla lettera a);

c) informazioni classificate fornite alla Corte dei conti europea da Stati terzi o organizzazioni internazionali recanti un contrassegno di classifica di sicurezza equivalente a uno dei contrassegni di classifica di sicurezza delle ICUE elencati alla lettera a), conformemente ai pertinenti accordi o intese amministrative sulla sicurezza delle informazioni.

3) La Corte dei conti tratta le informazioni di livello RESTREINT UE/EU RESTRICTED nei propri locali e adotta tutte le misure di protezione necessarie a tal fine. Sono adottate disposizioni affinché il personale della Corte dei conti che necessita di accedere a ICUE di livello più elevato possa farlo in idonei locali di altre istituzioni, agenzie o organismi dell'UE.

4) La presente decisione si applica a tutti i servizi e i locali della Corte dei conti.

5) Fatto salvo quando una disposizione riguarda gruppi specifici del personale, la presente decisione si applica ai Membri della Corte dei conti, al personale della Corte dei conti soggetto alla statuto dei funzionari e al regime applicabile agli agenti dell'Unione europea[2], agli esperti nazionali distaccati presso la Corte dei conti (END), ai prestatori di servizi e al loro personale, ai tirocinanti e a tutte le persone che hanno accesso agli edifici e ad altre risorse della Corte dei conti o alle informazioni gestite dalla stessa.

6) Salvo indicazione contraria, le disposizioni relative alle ICUE si applicano in modo equivalente alle informazioni classificate di cui al paragrafo 2, lettere b) e c), del presente articolo.

Articolo 2. **Definizioni**

Ai fini della presente decisione si intende per:

a) "autorizzazione di accesso alle ICUE", una decisione adottata dal direttore di Risorse umane, finanze e servizi generali della Corte dei conti sulla base dell'assicurazione data da un'autorità competente di uno Stato membro in base alla quale un funzionario o altro agente o END della Corte dei conti può, quando sia stata accertata la sua necessità di conoscere e una volta istruito sulle proprie responsabilità, avere accesso alle ICUE fino a un livello di classifica specifico (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore) e fino a una data stabilita; la persona in questione è indicata come in possesso del "nulla osta di sicurezza";

b) "classifica", l'attribuzione di un livello di riservatezza alle informazioni sulla base del grado di pregiudizio che la loro divulgazione non autorizzata potrebbe recare;

c) "materiale crittografico", algoritmi crittografici, moduli hardware e software crittografici e prodotti comprendenti dettagli di attuazione e documentazione associata e materiale di codifica;

d) "declassificazione", la soppressione di qualsiasi classifica di sicurezza;

---

[1] Cfr. l'accordo tra gli Stati membri dell'Unione europea, riuniti in sede di Consiglio, sulla protezione delle informazioni classificate scambiate nell'interesse dell'Unione europea, del 4 maggio 2011, e il relativo allegato (GU C 202 dell'8.7.2011, pag. 13).

[2] Regolamento n. 31 (CEE) relativo allo statuto dei funzionari e al regime applicabile agli altri agenti, come modificato, 01962R0031-1.1.2020-019.003-1 (https://eur-lex.europa.eu/eli/reg/1962/31 (1)/2020-01-01).

e) “documento”, qualsiasi informazione registrata, a prescindere dalla sua forma o dalle sue caratteristiche materiali;

f) “declassamento”, una riduzione del livello di classifica di sicurezza;

g) “nulla osta di sicurezza delle imprese”, una decisione amministrativa di un’autorità competente per la sicurezza, secondo la quale un’impresa è in grado, sotto il profilo della sicurezza, di offrire un adeguato livello di protezione alle ICUE di un determinato livello di classifica di sicurezza;

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

i) “detentore”, una persona debitamente autorizzata con una necessità di conoscere stabilita, che è in possesso di informazioni classificate ed è di conseguenza responsabile della loro protezione;

j) “autorità competente per la sicurezza delle informazioni”, il responsabile della sicurezza delle informazioni presso la Corte dei conti, che può delegare, in tutto o in parte, i compiti di cui alla presente decisione;

k) “informazione”, qualsiasi informazione scritta o orale indipendentemente da quale ne sia il supporto o l’autore;

l) “materiale”, qualsiasi mezzo, vettore di dati o elemento di macchinario o attrezzatura;

m) “originatore”, istituzione, agenzia o organismo dell’UE, Stato membro, paese terzo o organizzazione internazionale sotto la cui autorità sono state create e/o introdotte nelle strutture dell’UE informazioni classificate;

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

o) “certificato di nulla osta di sicurezza del personale” (PSCC), un certificato rilasciato dal direttore di Risorse umane, finanze e servizi generali presso la Corte dei conti attestante che una persona ha ottenuto il nulla osta di sicurezza o possiede un’autorizzazione di accesso alle ICUE in corso di validità, in cui figura il livello di ICUE cui detta persona può accedere (CONFIDENTIEL UE/EU CONFIDENTIAL o superiore), il periodo di validità di tale nulla osta o autorizzazione e la data di scadenza del certificato stesso;

p) “autorità competente per la sicurezza materiale”, il responsabile della sicurezza presso la Corte dei conti, al quale spetta l’attuazione delle misure e procedure di sicurezza materiale necessarie a proteggere le ICUE;

q) “cancelleria”, entità amministrata dal segretariato della Corte, ubicato in un settore amministrativo sotto la responsabilità del direttore di Risorse umane, finanze e servizi generali presso la Corte dei conti. È responsabile dell’ingresso e dell’uscita di informazioni di livello RESTREINT UE/EU RESTRICTED, o equivalente, scambiate con la Corte dei conti;

r) “ufficio di registrazione delle ICUE”, settore istituito all’interno di una zona protetta e gestito dal funzionario responsabile del controllo delle registrazioni, debitamente autorizzato e in possesso di nulla osta di sicurezza, presso la Corte dei conti. È responsabile dell’ingresso e dell’uscita di informazioni di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, oppure di un livello equivalente, scambiate con la Corte dei conti;

s) “autorità di accreditamento in materia di sicurezza”, il direttore di Risorse umane, finanze e servizi generali della Corte dei conti.

Articolo 3. **Misure per proteggere le ICUE**

1) La Corte dei conti provvede alla protezione di tutte le informazioni classificate in modo commensurato al livello di classifica determinato dall’originatore e conformemente alla presente decisione.

2) A tal fine, la Corte dei conti sottopone il trattamento delle ICUE a misure di sicurezza materiale e, ove opportuno, del personale, comprese autorizzazioni di accesso per le persone e le misure individuate per la protezione dei sistemi di comunicazione e informazione. Queste misure sono descritte agli articoli da 4 a 6 e si applicano per tutto il ciclo di vita delle ICUE. Sono commisurate alla classifica di sicurezza delle ICUE, alla forma e al volume delle informazioni o dei materiali, all’ubicazione e alla tipologia di costruzione delle strutture in cui sono conservate le ICUE e alla valutazione a livello locale della minaccia di attività dolose e/o criminose, compreso lo spionaggio, il sabotaggio e il terrorismo.

3) Le ICUE sono protette da misure di sicurezza materiale e le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono protette anche da misure di sicurezza del personale.

4) Le ICUE possono essere trasmesse solo alle persone che hanno necessità di conoscere, all’interno dell’istituzione. Il detentore di qualsiasi ICUE è tenuto a proteggerla conformemente alla presente decisione.

5) Le ICUE non devono essere divulgate né a voce né per iscritto. Le osservazioni preliminari, le relazioni, i pareri, i comunicati stampa e altri prodotti della Corte dei conti, il suo sito Internet e Intranet, gli interventi orali, le risposte alle domande di accesso ai documenti[3] e le registrazioni vocali o video non devono contenere o fare riferimento a ICUE o a loro estratti. Tuttavia, se l’originatore ha pubblicato documenti o informazioni un riferimento alle ICUE, tale riferimento può essere riportato.

6) In deroga al paragrafo 5, la Corte dei conti e l’originatore possono convenire che, nel caso di un audit specifico, la Corte dei conti può riprodurre o utilizzare elementi di ICUE in un documento. In tale evenienza, il documento della Corte dei conti è presentato in via preliminare all’originatore delle ICUE di cui trattasi, prima o durante la procedura in contraddittorio. In tali circostanze, la Corte dei conti e l’originatore decidono se classificare il documento prodotto dalla Corte dei conti stessa. Qualora un Membro relatore della Corte dei conti ritenga necessario comunicare una relazione di audit in tutto o in parte classificata a determinati destinatari presso il Parlamento europeo o il Consiglio, conto tenuto di tutte le misure di sicurezza associate alla presente decisione, occorre ottenere il consenso dell’originatore delle informazioni classificate. Il quadro giuridico e la procedura per lo scambio di tali documenti sono definiti all’articolo 7.

7) Se per l’esercizio del suo mandato è necessaria una più ampia condivisione di taluni elementi di un documento o informazione classificati, la Corte dei conti consulta l’originatore, tenendo in debito conto il contrassegno di classifica di sicurezza, prima di decidere di utilizzare tali elementi o informazioni, qualora ritenga che vi sia un interesse pubblico prevalente a farlo. Le

[3] Ai sensi della decisione n. 12-2005 della Corte dei conti relativa all’accesso del pubblico ai documenti della Corte dei conti, come modificata dalla decisione 14-2009 (GU C 67 del 20.3.2009, pag. 1).

informazioni sono utilizzate nella relazione soltanto in modo tale da non poter ledere gli interessi dell'originatore. Ciò potrebbe essere adeguatamente garantito chiedendo all'originatore di formulare osservazioni al fine di concordare le modalità di anonimizzazione, la condensazione o generalizzazione delle informazioni, ecc. e rispettare, al contempo, gli interessi dei soggetti principalmente toccati dalle informazioni pubblicate.

8) La Corte dei conti non trasmette ICUE a un'altra istituzione, agenzia, organo o ufficio dell'UE, uno Stato membro, un paese terzo o a un'organizzazione internazionale senza previa consultazione dell'originatore ed espresso consenso scritto.

9) Fatto salvo il caso in cui l'originatore di un documento classificato di livello di classifica SECRET UE / EU SECRET o inferiore abbia imposto restrizioni alla sua duplicazione o traduzione, tali documenti possono essere duplicati o tradotti su richiesta del detentore e conformemente alle istruzioni operative pratiche dell'autorità competente per la sicurezza delle informazioni presso la Corte dei conti. Le misure di sicurezza applicabili al documento originale si applicano anche alle copie e alle traduzioni.

10) Se la Corte dei conti ha la necessità che un documento classificato ricevuto, o a cui è autorizzata ad accedere, venga declassato o declassificato, la Corte consulta l'originatore per chiedergli di fornire una versione declassata o declassificata del documento.

Articolo 4. Sicurezza del personale

1) In virtù delle proprie funzioni, i Membri della Corte dei conti sono autorizzati ad accedere a tutte le ICUE e a partecipare a riunioni in cui sono trattate ICUE. I Membri sono informati dei loro obblighi in materia di sicurezza per quanto riguarda la protezione delle ICUE e riconoscono per iscritto la propria responsabilità di proteggere tali informazioni.

2) Un membro del personale della Corte dei conti, che sia funzionario, un effettivo soggetto al regime applicabile agli altri agenti o un END riceve accesso a ICUE solo una volta che:

   i. sia stata accertata la sua necessità di conoscere;

   ii. sia stato istruito sulle norme di sicurezza per la protezione delle ICUE, nonché sulle norme e gli orientamenti di sicurezza pertinenti, e abbia riconosciuto per iscritto la propria responsabilità di proteggere tali informazioni;

   iii. nel caso delle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL e superiore, abbia ottenuto il nulla osta di sicurezza e l'autorizzazione di accesso.

3) La procedura per determinare se un funzionario o un altro membro del personale della Corte dei conti possa essere autorizzato ad accedere a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, conto tenuto della lealtà, integrità e affidabilità del soggetto in questione, e dopo aver ricevuto dalle autorità competenti di uno Stato membro la garanzia di cui all'articolo 2, lettera n), viene stabilita in una decisione delegata adottata in conformità dell'articolo 10, paragrafo 10. La decisione di concedere l'autorizzazione di accesso è presa dal direttore di Risorse umane, finanze e servizi generali della Corte dei conti.

4) Il direttore di Risorse umane, finanze e servizi generali della Corte dei conti può rilasciare PSCC in cui è specificato il livello di classifica per il quale i soggetti possono avere accesso a ICUE (CONFIDENTIEL UE / EU CONFIDENTIAL o superiore), il periodo di validità della corrispondente autorizzazione di accesso e la data di scadenza del PSCC.

5) Solo i soggetti in possesso dell'autorizzazione di cui al precedente paragrafo 2, punto iii), e i Membri della Corte dei conti ai sensi del precedente paragrafo 1 possono partecipare a riunioni in cui sono trattate informazioni di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore. La Corte dei conti e l'originatore stabiliscono caso per caso le modalità pratiche di tali riunioni.

6) I servizi della Corte dei conti che sono responsabili dell'organizzazione di riunioni in cui vanno trattate informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore comunicano in tempo utile all'autorità competente per la sicurezza delle informazioni le date, gli orari e i luoghi delle riunioni, con le liste dei partecipanti.

7) Chi è in possesso di ICUE senza debita autorizzazione e/o senza una comprovata necessità di sapere deve riportare la situazione all'autorità competente per la sicurezza delle informazioni quanto prima e provvedere affinché le ICUE siano protette conformemente alla presente decisione.

Articolo 5. **Misure di sicurezza materiale per la protezione di informazioni classificate**

1) Per "sicurezza materiale" si intende il ricorso a misure di protezione materiali e tecniche volte a impedire l'accesso non autorizzato alle ICUE.

2) Le misure di sicurezza materiale sono intese a impedire a intrusi l'ingresso fraudolento o con la forza, a scoraggiare, ostacolare e scoprire azioni non autorizzate e a consentire la segregazione del personale per quanto riguarda il loro accesso alle ICUE in base al principio della necessità di conoscere. Tali misure sono stabilite sulla base di una procedura di gestione del rischio, ai sensi della presente decisione.

3) Le zone in cui sono trattate o conservate le ICUE sono sottoposte a ispezioni periodiche da parte dell'autorità competente per la sicurezza della Corte dei conti.

4) Per trattare e conservare le ICUE si utilizzano solo le apparecchiature o i dispositivi conformi alle norme applicabili in seno alle istituzioni, agenzie od organismi dell'UE per proteggere le ICUE.

5) Il personale della Corte dei conti può accedere a ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, oppure di livello equivalente, in zone protette al di fuori dei locali della Corte dei conti.

6) La Corte dei conti può concludere un accordo sul livello dei servizi con un'altra istituzione dell'UE a Lussemburgo al fine di poter trattare e conservare informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore in una zona protetta di tale istituzione. Salvo accordo specifico dell'originatore, tali ICUE non sono trattate o conservate nei locali della Corte dei conti e non sono duplicate o tradotte dalla Corte dei conti.

7) Le informazioni di livello RESTREINT UE/EU RESTRICTED ricevute sono iscritte nell'apposito registro dalla Corte dei conti. La consultazione di informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, oppure di livello equivalente, al di fuori dei locali della Corte dei conti è iscritta nell'apposito registro a fini di sicurezza.

8) Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED possono essere conservate in idonei mobili da ufficio chiusi a chiave, in una zona amministrativa o in una zona protetta. Le ICUE classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET sono conservate, nell'ambito di un accordo sul livello dei servizi, in un contenitore di sicurezza in una zona protetta di un'altra istituzione delle UE a Lussemburgo.

9) Al di fuori dell'ufficio di registrazione, le ICUE sono trasferite tra i servizi e i locali come segue:

a) di norma, le ICUE sono trasmesse con mezzi elettronici protetti mediante prodotti crittografici approvati conformemente all'articolo 6, paragrafo 8;

b) se non sono trasmesse secondo le modalità descritte al punto a), le ICUE sono trasferite utilizzando un supporto dati (ad esempio, una chiave USB, CD, disco rigido) protetto da prodotti crittografici approvati a norma dell'articolo 6, paragrafo 8, oppure come copia cartacea in una busta sigillata opaca.

10) Le informazioni di livello RESTREINT UE/EU RESTRICED possono essere distrutte dal detentore, fatte salve le norme di archiviazione applicabili presso la Corte dei conti. Le informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore sono distrutte soltanto dal funzionario responsabile del controllo delle registrazioni su richiesta del detentore oppure da un'autorità competente conformemente alle norme di archiviazione applicabili presso la Corte dei conti. I documenti classificati di livello SECRET UE/EU SECRET sono distrutti in presenza di un testimone con nulla osta di sicurezza corrispondente almeno al livello di classifica del documento da distruggere. Il responsabile del controllo delle registrazioni e il testimone, ove ne sia richiesta la presenza, firmano un certificato di distruzione che è archiviato presso l'ufficio di registrazione. Il responsabile del controllo delle registrazioni conserva gli atti della distruzione di documenti di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET per almeno cinque anni.

11) L'autorità competente per la sicurezza materiale e l'autorità competente per la sicurezza delle informazioni redigono un piano congiunto, che tenga conto delle circostanze locali, per salvaguardare le ICUE in tempi di crisi, in cui sono compresi all'occorrenza piani per la loro distruzione o rimozione in caso di emergenza. Impartiscono le istruzioni che ritengono opportune per impedire che le ICUE cadano nelle mani di persone non autorizzate.

12) Qualora le ICUE debbano essere trasportate fisicamente, la Corte dei conti osserva le misure imposte dall'originatore per proteggerle dalla divulgazione non autorizzata durante il trasporto.

13) Nell'allegato sono stabilite le misure di sicurezza materiale che si applicano nelle zone amministrative in cui sono trattate e conservate informazioni di livello RESTREINT UE/EU RESTRICTED.

Articolo 6. Protezione delle ICUE nei sistemi di comunicazione e informazione

1) Ai fini del presente articolo, per "sistema di comunicazione e informazione" si intende qualsiasi sistema che consente il trattamento delle ICUE in forma elettronica. Un sistema di comunicazione e informazione comprende tutte le risorse necessarie al suo funzionamento, ivi compresi l'infrastruttura, l'organizzazione, il personale e le risorse dell'informazione.

2) Per "utente legittimo" si intende un Membro, un funzionario, un altro agente o un END della Corte dei conti con una necessitò accertata e riconosciuta di accedere a uno specifico sistema di informazione.

3) La Corte dei conti fornisce garanzie che i propri sistemi proteggeranno le informazioni che trattano in misura adeguata e funzioneranno nel dovuto, a tempo debito, sotto il controllo degli utenti legittimi. A tal fine garantiscono livelli adeguati di:

- autenticità, ossia la garanzia che l'informazione è veritiera e proviene da fonti in buona fede;
- disponibilità, ossia la proprietà di accessibilità e utilizzabilità su richiesta di un'entità autorizzata;

- riservatezza, ossia la proprietà per cui l'informazione non è divulgata a persone, entità o procedure non autorizzate;
- integrità, ossia la proprietà di tutela della precisione e della completezza delle informazioni e delle risorse;
- non disconoscibilità, ossia la capacità di provare che un'azione o un evento sono effettivamente accaduti e non possono essere negati in seguito.

Tale garanzia si basa su una procedura di gestione del rischio. Per "rischio" si intende la possibilità che una data minaccia sfrutti le vulnerabilità interne ed esterne di un'organizzazione o di uno qualsiasi dei sistemi da essa utilizzati, arrecando pertanto danno all'organizzazione o ai suoi beni materiali o immateriali. È calcolato come una combinazione tra le probabilità del verificarsi delle minacce e il loro impatto. La procedura di gestione del rischio deve comprendere le seguenti fasi: identificazione della minaccia e della vulnerabilità, valutazione del rischio, trattamento del rischio, accettazione del rischio e comunicazione del rischio.

- Per "valutazione del rischio" si intende l'identificazione delle minacce e delle vulnerabilità e l'esecuzione della corrispondente analisi del rischio, ossia l'analisi della probabilità e dell'impatto.
- Per "trattamento del rischio" si intende la mitigazione, rimozione, riduzione (tramite un'opportuna combinazione di misure tecniche, materiali, organizzative o procedurali), trasferimento o controllo del rischio.
- L'"accettazione del rischio" consiste nel decidere di accettare la permanenza di un rischio residuo in seguito al trattamento del rischio.
- L'espressione "rischio residuo" designa il rischio che permane una volta attuate delle misure di sicurezza, dato che non tutte le minacce possono essere neutralizzate né tutte le vulnerabilità eliminate.
- Per "comunicazione del rischio" si intende l'opera di sensibilizzazione ai rischi condotta tra le comunità di utenti di un sistema di comunicazione e informazione, informando di tali rischi le autorità di approvazione e riferendo sugli stessi alle autorità operative.

4) Tutte le apparecchiature e i dispositivi elettronici utilizzati per il trattamento delle ICUE sono conformi alle norme applicabili per la protezione delle ICUE. È data preferenza alle apparecchiature e ai dispositivi che sono già stati accreditati da un'altra istituzione, agenzia od organismo dell'UE. I dispositivi sono garantiti come sicuri durante l'intero ciclo della loro vita.

5) Il sistema di comunicazione e informazione della Corte dei conti per il trattamento delle ICUE è accreditato da un'autorità idonea. A tal fine, la Corte dei conti stipula un accordo sul livello dei servizi con un'autorità di accreditamento di sicurezza di un'istituzione dell'UE che abbia la capacità di accreditare CIS che trattano ICUE, al fine di ricevere una dichiarazione di accreditamento per le informazioni di livello RESTREINT UE/EU RESTRICTED che possono essere trattate nel CIS della Corte dei conti e i termini e le condizioni di funzionamento corrispondenti. L'accordo sul livello dei servizi fa anche riferimento alle norme da applicare nel processo di accreditamento ed è concluso secondo la procedura di cui all'articolo 10, paragrafo 3.

6) Qualora la Corte dei conti debba istituire un proprio processo di accreditamento per il suo CIS, il processo è istituito con una decisione di delega quale indicata all'articolo 10, paragrafo 10, della presente decisione, conformemente alle norme per il processo di accreditamento per CIS che trattano ICUE in altre istituzioni, agenzie e organismi dell'UE.

7) Il proprietario del sistema CIS è il solo responsabile della preparazione dei fascicoli e della documentazione di accreditamento, in linea con le norme applicabili.

8) Qualora le ICUE siano protette mediante prodotti crittografici, la Corte dei conti accorda la preferenza a prodotti approvati dal Consiglio o dal segretario generale del Consiglio nella sua

funzione di autorità di approvazione degli apparati crittografici oppure, in alternativa, ai prodotti approvati da altre istituzioni, agenzie e organismi dell'UE per la protezione di ICUE.

9) Le informazioni di livello RESTREINT UE/EU RESTRICTED sono trattati esclusivamente su dispositivi elettronici (quali stazioni di lavoro, stampanti, fotocopiatrici) situati in una zona amministrativa o in una zona protetta. I dispositivi elettronici che trattano informazioni RESTREINT UE/EU RESTRICTED sono separati dalle altre reti informatiche e protetti mediante adeguate misure fisiche o tecniche.

10) Tutto il personale della Corte dei conti coinvolto nella progettazione, nello sviluppo, nel collaudo, nel funzionamento, nella gestione o nell'utilizzo di CIS che trattano ICUE notifica al responsabile della sicurezza delle informazioni ogni potenziale lacuna di sicurezza, incidente, violazione o compromissione della sicurezza che potrebbe avere conseguenze sulla protezione del CIS e/o delle ICUE in esso contenute.

Articolo 7. Procedura per lo scambio e l'accesso a informazioni classificate

1) Quando incombe loro l'obbligo in virtù dei trattati o degli atti giuridici adottati in forza dei trattati, le istituzioni, le agenzie, le organi e gli uffici dell'UE e le autorità nazionali concedono alla Corte dei conti, di propria iniziativa o su richiesta scritta del Presidente, del Membro o dei Membri relatori o del segretario generale, l'accesso alle ICUE secondo la procedura seguente.

2) Le domande di accesso sono inviate alle istituzioni interessate tramite la cancelleria della Corte dei conti.

3) Ove necessario, la Corte dei conti conclude un accordo amministrativo riguardante gli aspetti pratici dello scambio di ICUE o di informazioni equivalenti.

4) Ai fini della conclusione di tali accordi amministrativi, la Corte dei conti fornisce all'originatore tutte le informazioni necessarie sul proprio sistema di sicurezza delle informazioni. All'occorrenza, può essere organizzata una visita di valutazione.

5) Questi accordi amministrativi sono conclusi nel pieno rispetto del principio delle attribuzioni conferite e del principio di leale cooperazione di cui all'articolo 13 del trattato sull'Unione europea. Sono conclusi secondo la procedura di cui all'articolo 10, paragrafo 4.

6) Qualora non esista alcun accordo amministrativo con una data istituzione, organismo o agenzia dell'UE, un paese terzo od un'organizzazione internazionale per la trasmissione di informazioni classificate alla Corte dei conti, quest'ultima firma una dichiarazione d'impegno a proteggere le informazioni classificate che riceve.

Articolo 8. Violazione della sicurezza, perdita o compromissione di informazioni classificate

1) Per violazione della sicurezza si intende un atto o omissione da parte di un soggetto che viola le norme di sicurezza contenute nella presente decisione e nelle sue modalità di attuazione.

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

3) Qualsiasi violazione o sospetta violazione della sicurezza è immediatamente segnalata all'autorità competente per la sicurezza delle informazioni presso la Corte dei conti.

4) Qualora sia noto, o vi siano ragionevoli motivi per ritenere, che siano state compromesse o perdute ICUE, l'autorità competente per la sicurezza delle informazioni informa il direttore di

Risorse umane, finanze e servizi generali e il segretario generale della Corte dei conti. Il direttore di Risorse umane, finanze e servizi generali informa immediatamente la corrispondente autorità competente per la sicurezza presso l'originatore. Il suddetto direttore della Corte dei conti conduce un'indagine e comunica al segretario generale della Corte dei conti e all'autorità competente della sicurezza presso l'originatore l'esito raggiunto e le misure adottate per evitare che la situazione si ripeta. Qualora sia coinvolto un Membro della Corte dei conti, spetta al Presidente della Corte dei conti adottare provvedimenti in collaborazione con il segretario generale della Corte dei conti.

5) Un funzionario o altro agente della Corte dei conti responsabile di una violazione delle norme sulla sicurezza stabilite nella presente decisione e nelle sue modalità di attuazione è passibile delle sanzioni stabilite dallo statuto dei funzionari e dal regime applicabile agli altri agenti delle istituzioni dell'Unione europea.

6) Un Membro della Corte dei conti che non rispetta i termini della presente decisione è passibile dei provvedimenti e delle sanzioni di cui all'articolo 286, paragrafo 6, del TFUE.

7) Qualsiasi soggetto responsabile della compromissione o della perdita di ICUE è passibile di sanzioni disciplinari e/o azioni legali conformemente alle disposizioni legislative, normative e regolamentari applicabili.

Articolo 9. Sicurezza in caso di intervento esterno

1) La Corte dei conti può affidare a contraenti registrati in uno Stato membro, in virtù del contratto che li lega, l'esecuzione di compiti che comportano o richiedono l'accesso a ICUE. Ciò può avvenire, in particolare, in rapporto alla manutenzione dei sistemi di comunicazione e informazione e della rete informatica.

2) In caso di intervento esterno, la Corte dei conti adotta tutte le misure di sicurezza necessarie di cui al paragrafo 3 del presente articolo (fra cui la richiesta di un nulla osta di sicurezza delle imprese) per garantire che le ICUE siano protette da candidati e offerenti durante l'intera durata di una procedura di gara e di appalto, nonché da contraenti e subcontraenti per l'intera durata del contratto. L'amministrazione aggiudicatrice provvede affinché nei contratti siano menzionate le norme minime di sicurezza di cui alla presente decisione al fine di obbligare i contraenti a rispettarle.

3) Le norme di sicurezza, le procedure d'appalto, nonché i moduli e modelli per contratti e subcontratti che comportano l'accesso a ICUE, i bandi di gara, gli orientamenti sulle circostanze in cui è richiesto il nulla osta di sicurezza delle imprese e del personale, le istruzioni di sicurezza su programmi o progetti, le lettere sugli aspetti di sicurezza, le visite, nonché la trasmissione e il trasporto di ICUE ai sensi di tali contratti e subcontratti sono conformi alle norme, ai moduli e ai modelli stabiliti dalla Commissione europea per contratti classificati nella decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE.

Articolo 10. Attuazione della decisione e responsabilità connesse

1) I servizi della Corte dei conti adottano tutte le misure necessarie che rientrano nelle loro competenze per provvedere ad applicare, nel trattamento o nella conservazione delle ICUE o di altre informazioni classificate, la presente decisione e le pertinenti modalità di attuazione.

2) Il segretario generale è l'autorità che ha il potere di nomina e l'autorità abilitata a concludere contratti di assunzione per tutti i funzionari e gli altri agenti. Il segretario generale può delegare al direttore di Risorse umane, finanze e servizi generali la responsabilità di concedere ai

funzionari e agli altri agenti l'autorizzazione ad accedere a informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, di esercitare la sua funzione di autorità di accreditamento in materia di sicurezza e di vigilare sul segretariato della Corte per quanto concerne il trattamento delle ICUE.

3) Il segretario generale ha il potere di concludere accordi sul livello dei servizi per l'accreditamento delle apparecchiature e dei sistemi di comunicazione e informazione della Corte dei conti, per l'uso di una zona protetta in un'altra istituzione dell'UE e per la procedura relativa alle domande di nulla osta di sicurezza del personale per accedere a ICUE.

4) Il direttore di Risorse umane, finanze e servizi generali ha il potere di concludere accordi amministrativi con le istituzioni, agenzie e altri organismi dell'UE per lo scambio di ICUE, di cui la Corte dei conti necessita per l'espletamento del proprio mandato. Tale direttore può anche concludere accordi amministrativi con paesi terzi o organizzazioni internazionali sulla protezione di qualsiasi informazione classificata che riceve.

5) Il direttore di Risorse umane, finanze e servizi generali ha il potere di firmare dichiarazioni di impegno a proteggere le ICUE che vanno fornite nel contesto di una trasmissione ad hoc eccezionale.

6) Il responsabile della sicurezza delle informazioni della Corte dei conti svolge la funzione di autorità competente per la sicurezza delle informazioni. Il responsabile della sicurezza delle informazioni e i soggetti a cui delega in tutto o in parte i propri compiti dispongono del nulla osta di sicurezza adeguato. L'autorità competente per la sicurezza delle informazioni assume le proprie responsabilità in stretta collaborazione con la direzione Risorse umane, finanze e servizi generali, la direzione Informazione, ambiente di lavoro e innovazione e la direzione del Comitato per il controllo della qualità dell'audit (cfr. in particolare articoli 4, 6 e 8). Spetta inoltre all'autorità competente per la sicurezza delle informazioni organizzare corsi di formazione e incontri di sensibilizzazione sulla sicurezza delle informazioni, nonché condurre ispezioni periodiche per verificare il rispetto della presente decisione, anche in caso di intervento esterno, e degli eventuali provvedimenti da prendere per assicurarlo.

7) Il responsabile della sicurezza è responsabile delle misure di sicurezza materiale (con particolare riferimento all'articolo 5).

8) La cancelleria istituita presso il segretariato della Corte dei conti è il punto di ingresso e di uscita delle informazioni classificate di livello RESTREINT UE/EU RESTRICTED che la Corte dei conti può scambiare con altre istituzioni, agenzie e organismi dell'UE e con gli Stati membri. È inoltre il punto di ingresso e di uscita delle informazioni dei paesi terzi e delle organizzazioni internazionali di livello equivalente. La cancelleria è organizzata come stabilito in una decisione delegata. Il responsabile di tale ufficio assume le seguenti responsabilità principali:

   a) registrazione dell'ingresso e dell'uscita delle informazioni classificate a livello RESTREINT UE/EU RESTRICTED;

   b) gestione di apposite zone amministrative per la registrazione del trattamento, della conservazione e della consultazione di ICUE di livello RESTREINT UE/EU RESTRICTED.

9) Nell'ambito di un accordo sul livello dei servizi per l'uso di una zona protetta presso un'altra istituzione dell'UE viene istituito un ufficio di registrazione. L'ufficio di registrazione organizzato dal segretariato generale della Corte sotto la responsabilità del direttore di Risorse umane, finanze e servizi generali della Corte costituisce il punto di ingresso e di uscita delle informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore, che la Corte può scambiare con altre istituzioni, agenzie o organismi dell'UE e con gli Stati membri È inoltre il punto di ingresso e di uscita delle informazioni dei paesi terzi e delle organizzazioni internazionali di livello equivalente. È dotato di adeguate casseforti e altri dispositivi di

sicurezza idonei a proteggere informazioni classificate di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore. L'ufficio di registrazione è organizzato come stabilito in una decisione delegata. Il responsabile del controllo delle registrazioni dispone di un nulla osta di sicurezza adeguato e assume le seguenti responsabilità principali:

a) gestione delle operazioni relative alla registrazione, consultazione, conservazione, riproduzione, traduzione, trasmissione, invio e, se del caso, distruzione di ICUE;

b) assolvimento di altri compiti legati alla protezione delle ICUE stabiliti in una decisione delegata.

10) Il Comitato amministrativo adotta una decisione delegata che stabilisce le modalità di attuazione della presente decisione. Il responsabile della sicurezza delle informazioni redige orientamenti sulla sicurezza delle informazioni. Il Comitato per il controllo della qualità dell'audit redige orientamenti di audit.

Articolo 11. **Entrata in vigore**

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

Fatto a Lussemburgo, il 3 giugno 2021

Per la Corte dei conti

Klaus-Heiner Lehne
Presidente

Allegato: MISURE DI SICUREZZA MATERIALE RIGUARDANTI LE ZONE AMMINISTRATIVE PER LE ICUE

ALLEGATO

MISURE DI SICUREZZA MATERIALE RIGUARDANTI LE ZONE AMMINISTRATIVE PER LE ICUE

1) Il presente allegato contiene le modalità di applicazione dell'articolo 5 della decisione. Queste sono le norme minime per la protezione materiale delle zone amministrative per informazioni di livello RESTREINT UE/EU RESTRICTED alla Corte dei conti: zone designate per la registrazione, la conservazione e la consultazione delle informazioni classificate RESTREINT UE/EU RESTRICTED.

2) Le misure di sicurezza materiale nelle zone amministrative sono finalizzate a impedire l'accesso non autorizzato a dette zone realizzando le seguenti azioni:

   a) è stabilito un perimetro chiaramente delimitato che permette l'ispezione delle persone;

   b) l'accesso senza scorta è consentito solo ai soggetti debitamente autorizzati dall'autorità competenze per la sicurezza delle informazioni presso la Corte dei conti o un'altra autorità competente;

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

3) L'autorità competente per la sicurezza delle informazioni presso la Corte dei conti può in via eccezionale concedere l'accesso a persone non autorizzate, anche per effettuare lavori in una zona amministrativa, purché ciò non comporti l'accesso a ICUE, che rimangono sottochiave. Tale persone possono entrare solo se accompagnate e costantemente sorvegliate dall'autorità competente per la sicurezza delle informazioni o dal responsabile del controllo delle registrazioni.

4) L'autorità competente per la sicurezza delle informazioni stabilisce le procedure per la gestione delle chiavi e/o delle combinazioni per tutte le zone amministrative e i contenitori di sicurezza. Queste procedure sono finalizzate a prevenire l'accesso non autorizzato.

5) Le combinazioni sono conosciute a memoria dal minor numero possibile di persone che hanno necessità di conoscerle. Le combinazioni per i contenitori di sicurezza in cui sono conservate informazioni di livello RESTREINT UE/EU RESTRICTED devono essere cambiate:

   - alla ricezione di un nuovo contenitore di sicurezza;
   - in caso di sostituzione del personale che conosce la combinazione;
   - qualora la combinazione sia stata, o si sospetta che sia stata, compromessa;
   - se una serratura è stata oggetto di manutenzione o riparazione;
   - almeno ogni dodici mesi.

6) L'autorità competente per la sicurezza delle informazioni e il responsabile della sicurezza sono responsabili del rispetto delle presenti norme.