Consiglio dell'Unione europea

Bruxelles, 29 marzo 2022
(OR. en)

7670/22
ADD 3

Fascicolo interistituzionale: 2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PROPOSTA

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	22 marzo 2022
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2022) 119 final - ANNEX 3
Oggetto:	ALLEGATO della proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione

Si trasmette in allegato, per le delegazioni, il documento COM(2022) 119 final - ANNEX 3.

All.: COM(2022) 119 final - ANNEX 3

COMMISSIONE
EUROPEA

Bruxelles, 22.3.2022
COM(2022) 119 final

ANNEX 3

ALLEGATO

della

proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ALLEGATO III

Misure per la protezione materiale delle informazioni classificate UE ("ICUE")

Attrezzature e misure organizzative per la protezione materiale delle ICUE

1. Una zona amministrativa deve soddisfare i seguenti requisiti:

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

   b) garantire che le finestre che potrebbero consentire l'accesso visivo non autorizzato alle ICUE all'interno della zona siano opacizzate o dotate di tende, cortine o altre coperture;

   c) l'accesso senza scorta deve essere concesso solo alle persone debitamente autorizzate dall'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione;

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

2. Oltre ai requisiti di cui al punto 1, una zona protetta deve soddisfare i seguenti requisiti:

   a) avere un perimetro chiaramente delimitato e protetto attraverso cui sono sempre controllati gli ingressi e le uscite;

   b) essere priva di linee di comunicazione, telefoni o altri dispositivi di comunicazione ed attrezzature elettriche o elettroniche non autorizzati;

   c) essere dotata di un sistema di rilevamento delle intrusioni ("IDS") per il controllo dell'accesso e il monitoraggio in tempo reale, in combinazione con personale di sicurezza incaricato degli interventi;

   d) essere ispezionata al termine del normale orario di lavoro e a intervalli casuali al di fuori del normale orario di lavoro, tranne nel caso in cui sia occupata da personale di servizio 24 ore su 24 e vi sia installato un IDS per il monitoraggio in tempo reale;

   e) essere gestita da personale formato, controllato e munito di apposito nulla osta di sicurezza;

   f) disporre di procedure operative di sicurezza che stabiliscano i seguenti elementi:

      i) il livello delle ICUE che possono essere trattate, discusse e conservate nella zona;

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

      iii) le persone autorizzate ad accedere senza scorta alla zona in virtù di un'autorizzazione di accesso alle ICUE e di una necessità di conoscere;

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

      v) ogni altra misura e procedura pertinente.

3. Se l'ingresso in una zona protetta costituisce un accesso diretto alle informazioni classificate ivi conservate, la zona deve essere definita di categoria I e, in caso contrario, di categoria II.

Per entrambe le categorie di zone protette di cui al primo comma e in aggiunta ai requisiti di cui al punto 2, il servizio/funzionario di sicurezza dell'istituzione o dell'organo dell'Unione in questione deve indicare chiaramente il livello più elevato di classifica di sicurezza delle informazioni normalmente conservate nella zona e definire chiaramente un perimetro che permette l'ispezione delle persone e, se possibile, dei veicoli.

Le istituzioni e gli organi dell'Unione devono assicurarsi che le persone che accedono a una zona protetta soddisfino i seguenti criteri:

a) richiedono un'autorizzazione specifica ad entrare nella zona;

b) sono scortate in ogni momento;

c) sono munite di apposito nulla osta di sicurezza, a meno che non siano presi provvedimenti intesi a garantire che non sia possibile alcun accesso alle ICUE.

4. Le zone protette che vengono protette dall'ascolto indiscreto passivo e attivo devono essere designate zone protette tecnicamente. Oltre ai requisiti per le zone protette, si applicano i seguenti requisiti:

a) tali zone devono essere dotate di un IDS, essere chiuse a chiave se non occupate ed essere sorvegliate se occupate. Le chiavi devono essere gestite conformemente all'articolo 29, paragrafo 3;

b) tali zone devono essere regolarmente soggette a ispezioni materiali o tecniche, o ad entrambe, da parte dell'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione. Dette ispezioni devono essere inoltre effettuate dopo qualsiasi ingresso non autorizzato, effettivo o sospettato;

c) tali zone devono essere dotate di un'adeguata protezione acustica e TEMPEST.

5. Tutte le persone che entrano in zone protette tecnicamente devono soddisfare i requisiti di cui al punto 3.

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

7. Nelle zone protette devono essere costruite camere blindate. Una camera blindata è una stanza con una costruzione materiale rafforzata, per la quale l'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione approva le pareti, il pavimento, il soffitto, le finestre e le porte provviste di serratura. Le camere blindate devono offrire una protezione equivalente a un contenitore di sicurezza approvato per la conservazione di ICUE dello stesso livello di classifica.

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

8. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED devono essere trattate e conservate in una delle seguenti zone:

a) in una zona protetta;

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

c) all'esterno di una zona protetta o di una zona amministrativa purché il detentore si sia impegnato a osservare le misure compensative decise dall'autorità di sicurezza di ogni istituzione e organo dell'Unione.

9. Le ICUE classificate di livello RESTREINT UE/EU RESTRICTED devono essere conservate in mobili da ufficio chiusi a chiave, in una zona amministrativa o in una zona protetta. Esse possono essere temporaneamente conservate all'esterno di una zona protetta o di una zona amministrativa purché il detentore si sia impegnato a conservare i documenti interessati in idonei mobili da ufficio chiusi a chiave quando non sono letti o discussi.

10. Le istituzioni e gli organi dell'Unione possono trattare e conservare le informazioni di livello RESTREINT UE/EU RESTRICTED all'esterno dei loro siti purché le informazioni interessate siano protette adeguatamente. A tal fine, le istituzioni e gli organi dell'Unione devono osservare le misure di cui al punto 8, lettera c).

11. Le informazioni di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devono essere trattate e conservate in una delle seguenti zone:

    a) in una zona protetta;

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

    c) all'esterno di una zona protetta o di una zona amministrativa, se il volume e il tempo sono limitati e purché il detentore si sia impegnato a osservare le misure compensative decise dall'autorità di sicurezza dell'istituzione o dell'organo dell'Unione in questione. Il detentore delle ICUE deve inoltre prendere le seguenti misure:

        i) informare l'ufficio di registrazione competente del fatto che i documenti classificati sono trattati all'esterno di una zona protetta;

        ii) tenere il documento sempre sotto il proprio controllo.

12. Le informazioni di livello CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devono essere conservate in una zona protetta accreditata a tale livello dalla competente autorità di accreditamento di sicurezza dell'istituzione o dell'organo dell'Unione in questione, all'interno di un contenitore di sicurezza o di una camera blindata.

13. I documenti classificati di livello CONFIDENTIEL UE/EU CONFIDENTIAL o superiore possono essere copiati solo dall'ufficio di registrazione pertinente.

14. Le informazioni di livello TRES SECRET UE/EU TOP SECRET devono essere trattate e conservate in una zona protetta accreditata a tale livello. A tal fine, le istituzioni e gli organi dell'Unione possono concludere gli accordi necessari per utilizzare una zona protetta ospitata e accreditata al livello adeguato dall'autorità di accreditamento di sicurezza di un'altra istituzione o un altro organo dell'Unione.

15. Le informazioni di livello TRES SECRET UE/EU TOP SECRET devono essere conservate in una zona protetta, accreditata a tale livello dall'autorità di accreditamento di sicurezza dell'istituzione o dell'organo dell'Unione in questione, secondo una delle modalità seguenti:

    a) in un contenitore di sicurezza approvato dall'autorità di sicurezza di ogni istituzione e organo dell'Unione, con uno dei seguenti controlli supplementari:

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

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

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