



### Sommario

#### II Atti non legislativi

##### REGOLAMENTI

- ★ **Regolamento di esecuzione (UE) 2018/557 della Commissione, del 9 aprile 2018, che modifica il regolamento (UE) n. 641/2014 per quanto riguarda la comunicazione relativa all'aumento del massimale per il regime di pagamento unico per superficie di cui all'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013 del Parlamento europeo e del Consiglio** ..... 1

##### DECISIONI

- ★ **Decisione (PESC) 2018/558 del comitato politico e di sicurezza, del 20 marzo 2018, che proroga il mandato del capo della missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia) (EUBAM Libia/1/2018)** ..... 3
- ★ **Decisione (UE, Euratom) 2018/559 della Commissione, del 6 aprile 2018, che stabilisce le norme di attuazione dell'articolo 6 della decisione (EU, Euratom) 2017/46 sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea** ..... 4
- ★ **Decisione di esecuzione (UE) 2018/560 della Commissione, del 10 aprile 2018, che modifica l'allegato della decisione di esecuzione (UE) 2017/247 relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri [notificata con il numero C(2018) 2191] <sup>(1)</sup>** ..... 11

<sup>(1)</sup> Testo rilevante ai fini del SEE.



## II

(Atti non legislativi)

## REGOLAMENTI

## REGOLAMENTO DI ESECUZIONE (UE) 2018/557 DELLA COMMISSIONE

del 9 aprile 2018

**che modifica il regolamento (UE) n. 641/2014 per quanto riguarda la comunicazione relativa all'aumento del massimale per il regime di pagamento unico per superficie di cui all'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013 del Parlamento europeo e del Consiglio**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 1307/2013 del Parlamento europeo e del Consiglio, del 17 dicembre 2013, recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune e che abroga il regolamento (CE) n. 637/2008 del Consiglio e il regolamento (CE) n. 73/2009 del Consiglio <sup>(1)</sup>, in particolare l'articolo 36, paragrafo 4,

considerando quanto segue:

- (1) Il regolamento di esecuzione (UE) n. 641/2014 della Commissione <sup>(2)</sup> stabilisce le modalità di applicazione del regolamento (UE) n. 1307/2013 recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune.
- (2) Il regolamento (UE) n. 1307/2013 è stato modificato dal regolamento (UE) 2017/2393 del Parlamento europeo e del Consiglio <sup>(3)</sup>, che, tra l'altro, ha aggiunto all'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013 la possibilità per gli Stati membri che applicano il regime di pagamento unico per superficie di aumentarne il massimale.
- (3) In considerazione delle modifiche apportate all'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013, è necessario stabilire norme per la comunicazione dell'aumento del massimale per il regime di pagamento unico per superficie.
- (4) È pertanto opportuno modificare di conseguenza il regolamento di esecuzione (UE) n. 641/2014.
- (5) Le misure di cui al presente regolamento sono conformi al parere del comitato per i pagamenti diretti,

<sup>(1)</sup> GUL 347 del 20.12.2013, pag. 608.

<sup>(2)</sup> Regolamento di esecuzione (UE) n. 641/2014 della Commissione, del 16 giugno 2014, recante modalità di applicazione del regolamento (UE) n. 1307/2013 del Parlamento europeo e del Consiglio recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune (GUL 181 del 20.6.2014, pag. 74).

<sup>(3)</sup> Regolamento (UE) 2017/2393 del Parlamento europeo e del Consiglio, del 13 dicembre 2017, che modifica i regolamenti (UE) n. 1305/2013 sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR), (UE) n. 1306/2013 sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune, (UE) n. 1307/2013 recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune, (UE) n. 1308/2013 recante organizzazione comune dei mercati dei prodotti agricoli e (UE) n. 652/2014 che fissa le disposizioni per la gestione delle spese relative alla filiera alimentare, alla salute e al benessere degli animali, alla sanità delle piante e al materiale riproduttivo vegetale (GUL 350 del 29.12.2017, pag. 15).

HA ADOTTATO IL PRESENTE REGOLAMENTO:

*Articolo 1*

**Modifica del regolamento di esecuzione (UE) n. 641/2014**

Nel regolamento di esecuzione (UE) n. 641/2014 è inserito il seguente articolo 16 bis:

«Articolo 16 bis

**Comunicazione relativa all'aumento del massimale per il regime di pagamento unico per superficie di cui all'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013**

Quando lo Stato membro comunica alla Commissione le proprie decisioni a norma dell'articolo 36, paragrafo 4, del regolamento (UE) n. 1307/2013, le informazioni da trasmettere alla Commissione sono le percentuali dei massimali nazionali annui figuranti nell'allegato II del medesimo regolamento, una volta dedotto l'importo derivante dall'applicazione dell'articolo 47, paragrafo 1, del medesimo regolamento per ogni anno civile dal 2018 al 2020.».

*Articolo 2*

**Entrata in vigore**

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

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

Fatto a Bruxelles, il 9 aprile 2018

*Per la Commissione*

*Il presidente*

Jean-Claude JUNCKER

---

## DECISIONI

### DECISIONE (PESC) 2018/558 DEL COMITATO POLITICO E DI SICUREZZA

del 20 marzo 2018

#### che proroga il mandato del capo della missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia) (EUBAM Libia/1/2018)

IL COMITATO POLITICO E DI SICUREZZA,

visto il trattato sull'Unione europea, in particolare l'articolo 38, terzo comma,

vista la decisione 2013/233/PESC del Consiglio, del 22 maggio 2013, sulla missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia) <sup>(1)</sup>, in particolare l'articolo 9, paragrafo 1,

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

considerando quanto segue:

- (1) Conformemente all'articolo 9, paragrafo 1, della decisione 2013/233/PESC, il comitato politico e di sicurezza (CPS) è autorizzato, a norma dell'articolo 38 del trattato, a prendere le decisioni appropriate al fine di esercitare il controllo politico e la direzione strategica della missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia), compresa quella relativa alla nomina del capomissione.
- (2) Il 18 luglio 2017 il CPS ha adottato la decisione (PESC) 2017/1401 <sup>(2)</sup> che proroga il mandato del sig. Vincenzo TAGLIAFERRI quale capo della missione EUBAM Libia dal 22 agosto 2017 al 21 agosto 2018.
- (3) Il 17 luglio 2017 il Consiglio ha adottato la decisione (PESC) 2017/1342 <sup>(3)</sup> recante modifica della decisione 2013/233/PESC e che proroga l'applicazione di tale decisione fino al 31 dicembre 2018.
- (4) Il 26 febbraio 2018 l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza ha proposto di prorogare il mandato del sig. Vincenzo TAGLIAFERRI quale capo della missione EUBAM Libia dal 22 agosto 2018 al 31 dicembre 2018,

HA ADOTTATO LA PRESENTE DECISIONE:

#### *Articolo 1*

Il mandato del sig. Vincenzo TAGLIAFERRI quale capo della missione EUBAM Libia è prorogato dal 22 agosto 2018 al 31 dicembre 2018.

#### *Articolo 2*

La presente decisione entra in vigore il 21 agosto 2018.

Fatto a Bruxelles, il 20 marzo 2018

*Per il comitato politico e di sicurezza*

*Il presidente*

W. STEVENS

---

<sup>(1)</sup> GUL 138 del 24.5.2013, pag. 15.

<sup>(2)</sup> Decisione (PESC) 2017/1401 del comitato politico e di sicurezza, del 18 luglio 2017, che proroga il mandato del capo della missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia) (EUBAM Libia/1/2017) (GU L 199 del 29.7.2017, pag. 13).

<sup>(3)</sup> Decisione (PESC) 2017/1342 del Consiglio, del 17 luglio 2017, recante modifica e proroga della decisione 2013/233/PESC sulla missione dell'Unione europea di assistenza alla gestione integrata delle frontiere in Libia (EUBAM Libia) (GU L 185 del 18.7.2017, pag. 60).

**DECISIONE (UE, Euratom) 2018/559 DELLA COMMISSIONE****del 6 aprile 2018****che stabilisce le norme di attuazione dell'articolo 6 della decisione (EU, Euratom) 2017/46 sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 249,

visto il trattato che istituisce la Comunità europea dell'energia atomica,

vista la decisione (UE, Euratom) 2017/46 della Commissione del 10 gennaio 2017 sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea <sup>(1)</sup>, in particolare l'articolo 6,

considerando quanto segue:

- (1) A seguito dell'adozione della decisione (UE, Euratom) 2017/46 è necessario che la Commissione riesami, aggiorni e consolidi le norme di attuazione della decisione C(2006)3602 della Commissione sulla sicurezza dei sistemi di comunicazione e informazione utilizzati dalla Commissione, ora abrogata.
- (2) Al membro della Commissione responsabile della Sicurezza è conferito, nel pieno rispetto delle norme e procedure interne, il potere di stabilire norme di attuazione in conformità all'articolo 13 della decisione (UE, Euratom) 2017/46 <sup>(2)</sup>.
- (3) È opportuno, pertanto, abrogare le norme di attuazione della decisione C(2006)3602,

HA ADOTTATO LA PRESENTE DECISIONE:

CAPO 1

**DISPOSIZIONI GENERALI***Articolo 1***Oggetto e ambito di applicazione**

1. L'oggetto e l'ambito di applicazione della presente decisione figurano all'articolo 1 della decisione (UE, Euratom) 2017/46.
2. Le disposizioni della presente decisione si applicano a tutti i sistemi di comunicazione e informazione (CIS). Tuttavia, le responsabilità definite nella presente decisione non si applicano ai CIS che elaborano le informazioni classificate UE. Le pertinenti responsabilità per questi sistemi sono determinate dal proprietario del sistema e dall'autorità di sicurezza della Commissione, conformemente alla decisione (UE, Euratom) 2015/444 <sup>(3)</sup>.
3. Il capo 2 della presente decisione presenta il quadro dell'attuazione pratica dell'organizzazione e delle responsabilità relative alla sicurezza informatica. Il capo 3 della presente decisione presenta il quadro dei processi attinenti all'articolo 6 della decisione (UE, Euratom) 2017/46 della Commissione.

*Articolo 2***Definizioni**

Alla presente decisione si applicano le definizioni di cui all'articolo 2 della decisione (UE, Euratom) 2017/46. Ai fini della presente decisione si applicano inoltre le seguenti definizioni:

1. «autorità di approvazione degli apparati crittografici» (CAA), funzione assunta dall'autorità di sicurezza della Commissione posta sotto l'autorità del direttore generale delle Risorse umane e della sicurezza;

<sup>(1)</sup> GUL 6 dell'11.1.2017, pag. 40.

<sup>(2)</sup> Decisione C(2017) 7428 della Commissione dell'8 novembre 2017 che conferisce il potere di adottare norme di attuazione, norme e orientamenti relativi alla sicurezza dei sistemi di comunicazione e informazione utilizzati dalla Commissione europea.

<sup>(3)</sup> Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GUL 72 del 17.3.2015, pag. 53).

2. «connessione a una rete esterna», qualsiasi connessione per le comunicazioni elettroniche tra la rete interna della Commissione e qualsiasi altra rete, compreso Internet. Da questa definizione sono escluse le reti di terzi che, da contratto, sono fornite per essere integrate nella rete interna della Commissione;
3. «deposito della chiave presso terzi (key escrow)», procedura per l'archiviazione di copie delle chiavi crittografiche presso una o più parti separate, che garantisce la separazione delle funzioni, per consentirne il recupero qualora venga persa la copia operativa. Le chiavi possono essere divise in due o più parti, ciascuna delle quali è depositata presso una parte diversa per garantire che nessuna delle parti posseda da sola l'intera chiave;
4. «RASCI», acronimo per la distribuzione delle responsabilità basata sui seguenti indicatori di attribuzione:
  - a) «responsabile» (responsible, R): che ha l'obbligo di agire e prendere decisioni per conseguire i risultati richiesti;
  - b) «tenuto a rispondere» (accountable, A): che deve rendere conto di azioni, decisioni e prestazioni;
  - c) «tenuto a fornire un sostegno» (supports, S): che ha l'obbligo di cooperare con la persona responsabile di eseguire il compito;
  - d) «consultato» (consulted, C): che è consultato per fornire consigli o pareri;
  - e) «informato» (informed, I): che è tenuto al corrente delle pertinenti informazioni.

## CAPO 2

### ORGANIZZAZIONE E RESPONSABILITÀ

#### Articolo 3

#### **Ruoli e responsabilità**

I ruoli e le responsabilità relativi agli articoli da 4 a 8 della presente decisione sono definiti nell'allegato in conformità al modello RASCI.

#### Articolo 4

#### **Allineamento alla politica in materia di sicurezza informatica della Commissione**

1. La direzione generale Risorse umane e sicurezza riesamina la politica di sicurezza informatica della Commissione e le norme e gli orientamenti relativi, per garantirne la conformità alle politiche generali di sicurezza della Commissione, in particolare la decisione (UE, Euratom) 2015/443 della Commissione <sup>(1)</sup> e la decisione (UE, Euratom) 2015/444.
2. Su richiesta di altri servizi della Commissione la direzione generale Risorse umane e sicurezza può riesaminarne le politiche di sicurezza informatica o altra documentazione sulla sicurezza informatica per assicurarne la conformità alla politica di sicurezza informatica della Commissione. Il capo del servizio della Commissione interessato si assicura che siano rimosse le eventuali incoerenze.
3. In quanto responsabile per la sicurezza delle informazioni, la direzione generale Risorse umane e sicurezza coopera con la direzione generale dell'Informatica per garantire che i processi di sicurezza informatica tengano pienamente conto della classificazione e dei principi di sicurezza di cui alla decisione (UE, Euratom) 2015/443, in particolare gli articoli 3 e 9.

## CAPO 3

### PROCESSI DI SICUREZZA INFORMATICA

#### Articolo 5

#### **Tecnologie di crittografia**

1. L'uso di tecnologie di crittografia per la protezione delle informazioni classificate UE (ICUE) è conforme alla decisione (UE, Euratom) 2015/444.
2. Le decisioni relative all'uso delle tecnologie di crittografia per la protezione dei dati non ICUE sono adottate dal proprietario del sistema di ciascun CIS, tenendo conto sia dei rischi che si vogliono ridurre grazie alla crittografia sia dei rischi che l'uso della crittografia comporta.
3. L'approvazione preventiva della CAA è richiesta per tutti gli usi delle tecnologie di crittografia, a meno che la crittografia sia utilizzata esclusivamente per proteggere la riservatezza dei dati non ICUE in transito e utilizzi protocolli standard per le comunicazioni di rete.

<sup>(1)</sup> Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

4. Con l'eccezione di cui al paragrafo 3, i servizi della Commissione si assicurano che copie di backup di tutte le chiavi di decriptazione siano depositate presso terzi allo scopo di recuperare le informazioni memorizzate nel caso in cui la chiave di decriptazione non sia disponibile. Il recupero dei dati criptati utilizzando i backup delle chiavi di decriptazione viene effettuato solo previa autorizzazione in conformità alla norma definita dalla CAA.
5. Le domande di approvazione dell'uso delle tecnologie di crittografia sono formalmente documentate e includono tutte le informazioni sul CIS e i dati da proteggere, le tecnologie da usare e le relative procedure operative di sicurezza. Le domande di approvazione sono firmate dal proprietario del sistema.
6. Le domande di approvazione dell'uso delle tecnologie di crittografia sono valutate dalla CAA in conformità alle norme e ai requisiti pubblicati.

#### Articolo 6

### Ispezioni sulla sicurezza informatica

1. La direzione generale Risorse umane e sicurezza effettua ispezioni sulla sicurezza informatica per verificare che le misure di sicurezza informatica siano conformi alle politiche di sicurezza informatica della Commissione e accertarsi dell'integrità di tali misure di controllo.
2. La direzione generale Risorse umane e sicurezza può effettuare un'ispezione sulla sicurezza informatica:
  - a) di propria iniziativa;
  - b) su richiesta del comitato direttivo per la sicurezza dell'informazione (ISSB);
  - c) su richiesta pervenuta da un proprietario del sistema;
  - d) a seguito di un incidente di sicurezza informatica; oppure
  - e) qualora sia stato individuato un rischio elevato per un particolare sistema.
3. I proprietari dei dati possono richiedere che sia effettuata un'ispezione sulla sicurezza informatica prima di archiviare le loro informazioni in un CIS.
4. I risultati dell'ispezione sono documentati in una relazione ufficiale inviata al proprietario del sistema, con copia al responsabile della sicurezza informatica a livello locale (LISO), contenente le risultanze e le raccomandazioni per migliorare la conformità del CIS alla politica di sicurezza informatica. La direzione generale Risorse umane e sicurezza riferisce all'ISSB in merito ai principali problemi e alle raccomandazioni formulate.
5. La direzione generale Risorse umane e sicurezza verifica l'attuazione delle raccomandazioni.
6. Laddove opportuno, le ispezioni sulla sicurezza informatica comprendono l'ispezione di servizi, locali e apparecchiature fornite al proprietario del sistema, e riguardano i fornitori di servizi sia interni sia esterni.

#### Articolo 7

### Accesso dalle reti esterne

1. La direzione generale Risorse umane e sicurezza fissa le regole in una norma sull'autorizzazione dell'accesso tra i CIS della Commissione e le reti esterne.
2. Tali regole operano una distinzione tra i diversi tipi di connessioni da reti esterne e stabiliscono appropriate regole di sicurezza per ciascun tipo di connessione, precisando anche se è necessaria la previa autorizzazione dell'autorità competente, come indicato al paragrafo 4.
3. Se necessario, l'autorizzazione viene concessa sulla base di una richiesta e di un processo di approvazione formali. L'approvazione è valida per una durata determinata e deve essere ottenuta prima di attivare la connessione.
4. La direzione generale Risorse umane e sicurezza ha la responsabilità generale di autorizzare le domande, ma può, ai sensi dell'articolo 17, paragrafo 3, della decisione (EU/Euratom) 2015/443, delegare, a propria discrezione, la responsabilità di autorizzare alcuni tipi di connessioni, fatte salve le condizioni di cui al paragrafo 8.
5. L'entità che rilascia l'autorizzazione può imporre requisiti di sicurezza aggiuntivi come prerequisito per l'approvazione al fine di proteggere il CIS e le reti della Commissione dai rischi di accesso non autorizzato e altre violazioni della sicurezza.

6. La direzione generale dell'Informatica è il fornitore abituale di servizi di rete per la Commissione. Ogni altro servizio della Commissione che utilizza una rete non fornita dalla direzione generale dell'Informatica ottiene la previa autorizzazione dell'ISSB. Il servizio della Commissione documenta la giustificazione commerciale alla base della richiesta e dimostra che i controlli sulla rete sono sufficienti per rispettare i requisiti di verifica dei flussi di informazioni in entrata e in uscita.
7. Il proprietario del sistema del CIS stabilisce i requisiti di sicurezza per l'accesso esterno a tale CIS e garantisce, con il sostegno del LISO, l'attuazione di adeguate misure per proteggerne la sicurezza.
8. Le misure di sicurezza attuate per le connessioni da rete esterna si basano sui principi della necessità di conoscere e del privilegio minimo, in virtù dei quali i singoli ricevono esclusivamente le informazioni e i diritti di accesso necessari all'espletamento dei loro incarichi ufficiali per la Commissione.
9. Tutte le connessioni da rete esterna sono filtrate e monitorate per individuare potenziali violazioni della sicurezza.
10. Quando le connessioni sono stabilite per consentire l'esternalizzazione di un CIS, l'autorizzazione è subordinata al positivo completamento della procedura di cui all'articolo 8.

#### Articolo 8

##### **Esternalizzazione dei CIS**

1. Ai fini della presente decisione un CIS si considera esternalizzato quando viene fornito sulla base di un contratto con un appaltatore terzo in virtù del quale il CIS è ospitato in locali non appartenenti alla Commissione. L'esternalizzazione riguarda uno o più CIS o altri servizi informatici e centri dati situati in locali non appartenenti alla Commissione e la gestione di dataset della Commissione da parte di servizi esterni.
  2. Nell'esternalizzare un CIS si tiene conto della sensibilità o della classificazione delle informazioni trattate, secondo le seguenti modalità:
    - a) i CIS che elaborano le ICUE sono accreditati in conformità alla decisione (UE, Euratom) 2015/444, previa consultazione dell'autorità di accreditamento in materia di sicurezza della Commissione. I sistemi che elaborano le ICUE non sono esternalizzati;
    - b) il proprietario del sistema del CIS che elabora informazioni non ICUE applica misure proporzionate per soddisfare le esigenze di sicurezza in conformità ai pertinenti obblighi giuridici o alla sensibilità delle informazioni, tenendo conto dei rischi dell'esternalizzazione. La direzione generale Risorse umane e sicurezza può imporre requisiti supplementari;
    - c) i progetti di sviluppo esternalizzati tengono conto della sensibilità del codice sviluppato e di eventuali dati delle prove utilizzati nella fase di sviluppo.
  3. In aggiunta ai principi di cui all'articolo 3 della decisione (UE, Euratom) 2017/46, ai CIS esternalizzati si applicano i seguenti principi:
    - a) gli accordi di esternalizzazione sono formulati in modo tale da evitare la dipendenza da specifici fornitori;
    - b) le disposizioni di sicurezza relative all'esternalizzazione riducono al minimo le possibilità che il personale di terzi abbia accesso alle informazioni della Commissione o le modifichi;
    - c) il personale che ha accesso al CIS esternalizzato sottoscrive un accordo di riservatezza;
    - d) l'esternalizzazione del CIS viene registrata nell'inventario dei CIS.
  4. Il proprietario del sistema, con la partecipazione del proprietario dei dati:
    - a) verifica e documenta i rischi connessi con l'esternalizzazione;
    - b) stabilisce i pertinenti requisiti di sicurezza;
    - c) si consulta con i proprietari dei sistemi di tutti gli altri CIS connessi per garantire che siano inclusi i loro requisiti di sicurezza;
    - d) si assicura che nel contratto di esternalizzazione siano inclusi adeguati requisiti e diritti di sicurezza;
    - e) rispetta tutti gli altri requisiti previsti dalla procedura dettagliata di cui al paragrafo 8.
- Questi interventi devono essere completati prima della firma del contratto o altro accordo di esternalizzazione di uno o più CIS.

5. I proprietari dei sistemi gestiscono i rischi connessi con l'esternalizzazione durante la durata di vita del CIS al fine di ottemperare ai requisiti di sicurezza definiti.
6. I proprietari dei sistemi si assicurano che gli appaltatori terzi siano tenuti a notificare immediatamente alla Commissione tutti gli incidenti di sicurezza informatica che interessano un CIS della Commissione esternalizzato.
7. Il proprietario del sistema è responsabile di garantire la conformità del CIS, del contratto di esternalizzazione e delle disposizioni di sicurezza alle norme della Commissione in materia di sicurezza delle informazioni e sicurezza informatica.
8. La direzione generale Risorse umane e sicurezza stabilisce una norma dettagliata relativa alle responsabilità e attività di cui ai punti da 1) a 7), in conformità all'articolo 10.

#### CAPO 4

### DISPOSIZIONI VARIE E FINALI

#### Articolo 9

#### Trasparenza

La presente decisione è resa nota al personale della Commissione e a tutte le persone cui si applica, ed è pubblicata nella *Gazzetta ufficiale dell'Unione europea*.

#### Articolo 10

#### Norme

1. Laddove necessario, le disposizioni della presente decisione sono ulteriormente specificate in norme e/o orientamenti in conformità alla decisione (UE, Euratom) 2017/46 e alla decisione C(2017)7428.. Le norme e gli orientamenti in materia di sicurezza informatica forniscono ulteriori dettagli sulle presenti norme di attuazione e sulla decisione (UE, Euratom) 2017/46 in relazione ad ambiti di sicurezza specifici in conformità alla norma ISO 27001:2013, allegato A. Tali norme e orientamenti si basano sulle migliori pratiche del settore e sono selezionati in modo da essere compatibili con l'ambiente informatico della Commissione.
2. Se necessario, e in conformità alla norma ISO 27001:2013, allegato A, sono elaborate norme attinenti agli ambiti di seguito specificati:
  - 1) organizzazione della sicurezza informatica;
  - 2) sicurezza delle risorse umane;
  - 3) gestione di attività;
  - 4) controllo dell'accesso;
  - 5) crittografia;
  - 6) sicurezza fisica e dell'ambiente;
  - 7) sicurezza operativa;
  - 8) sicurezza delle comunicazioni;
  - 9) acquisizione, sviluppo e manutenzione di sistemi;
  - 10) relazioni con i fornitori;
  - 11) gestione degli incidenti relativi alla sicurezza informatica;
  - 12) aspetti della sicurezza informatica attinenti alla gestione della continuità operativa;
  - 13) conformità.
3. L'ISSB approva le norme di cui ai paragrafi 1 e 2 prima della loro adozione.
4. Sono abrogate le norme di attuazione della decisione C(2006)3602 attinenti all'ambito di applicazione della presente decisione.
5. Le norme e gli orientamenti adottati a norma della decisione C(2006)3602 del 16 agosto 2006 rimangono in vigore nella misura in cui non siano in contrasto con le presenti norme di attuazione e fino a quando siano abrogati o sostituiti da norme o orientamenti da adottare ai sensi dell'articolo 13 della decisione (UE, Euratom) 2017/46.

---

*Articolo 11***Entrata in vigore**

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

Fatto a Bruxelles, il 6 aprile 2018

*Per la Commissione,  
a nome del presidente  
Günther OETTINGER  
Membro della Commissione*

---

## ALLEGATO

## RUOLI E RESPONSABILITÀ (RASCI)

Il modello RASCI assegna i ruoli alle entità utilizzando le seguenti abbreviazioni:

- a) R — Responsabile (Responsible)
- b) A — Tenuto a rispondere (Accountable)
- c) S — Tenuto a fornire un sostegno (Supporting)
- d) C — Consultato (Consulted)
- e) I — Informato (Informed)

Processo \ Ruolo	ISSB	HR (DS)	Commis- sione Servizi	Proprietario del sistema	Proprietario dei dati	LISO	DIGIT	Appaltatori
Allineamento alla politica in materia di sicurezza informatica della Commissione		<b>R/A</b>	<b>S</b>				<b>S</b>	
Tecnologie di crittografia		<b>C</b>	<b>A</b>	<b>R</b>	<b>I</b>	<b>C</b>		
Ispezioni di sicurezza informatica	<b>I</b>	<b>A/R</b>		<b>S</b>	<b>I</b>	<b>I</b>	<b>S</b>	
Accesso dalle reti esterne	<b>C</b> <sup>(1)</sup>	<b>C</b>	<b>A</b>	<b>R</b>	<b>I</b>	<b>S</b>	<b>S</b>	
Esternalizzazione dei CIS		<b>S/C</b>	<b>A</b>	<b>R/C</b> <sup>(2)</sup>	<b>S</b>	<b>C</b>		<b>S</b>

<sup>(1)</sup> L'ISSB è consultato in relazione al funzionamento delle reti interne da qualsiasi servizio della Commissione che non sia la direzione generale dell'Informatica.

<sup>(2)</sup> Responsabile è il proprietario del sistema del CIS che viene esternalizzato, mentre è consultato il proprietario del sistema di qualsiasi altro CIS interconnesso con il CIS esternalizzato.

**DECISIONE DI ESECUZIONE (UE) 2018/560 DELLA COMMISSIONE****del 10 aprile 2018****che modifica l'allegato della decisione di esecuzione (UE) 2017/247 relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri***[notificata con il numero C(2018) 2191]***(Testo rilevante ai fini del SEE)**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva 89/662/CEE del Consiglio, dell'11 dicembre 1989, relativa ai controlli veterinari applicabili negli scambi intracomunitari, nella prospettiva della realizzazione del mercato interno <sup>(1)</sup>, in particolare l'articolo 9, paragrafo 4,vista la direttiva 90/425/CEE del Consiglio, del 26 giugno 1990, relativa ai controlli veterinari e zootecnici applicabili negli scambi intracomunitari di taluni animali vivi e prodotti di origine animale, nella prospettiva della realizzazione del mercato interno <sup>(2)</sup>, in particolare l'articolo 10, paragrafo 4,

considerando quanto segue:

- (1) La decisione di esecuzione (UE) 2017/247 della Commissione <sup>(3)</sup> è stata adottata a seguito della comparsa di focolai di influenza aviaria ad alta patogenicità del sottotipo H5 in vari Stati membri («gli Stati membri interessati») e all'istituzione di zone di protezione e sorveglianza da parte delle autorità competenti degli Stati membri interessati in conformità dell'articolo 16, paragrafo 1, della direttiva 2005/94/CE del Consiglio <sup>(4)</sup>.
- (2) La decisione di esecuzione (UE) 2017/247 stabilisce che le zone di protezione e sorveglianza istituite dalle autorità competenti degli Stati membri interessati in conformità della direttiva 2005/94/CE devono comprendere almeno le zone elencate come zone di protezione e sorveglianza nell'allegato di tale decisione di esecuzione. Essa prevede altresì che le misure da applicarsi nelle zone di protezione e sorveglianza, secondo quanto stabilito dall'articolo 29, paragrafo 1, e dall'articolo 31 della direttiva 2005/94/CE, siano mantenute almeno fino alle date stabilite per tali zone indicate nell'allegato della medesima decisione di esecuzione.
- (3) Dalla data della sua adozione la decisione di esecuzione (UE) 2017/247 è stata modificata diverse volte per tenere conto degli sviluppi della situazione epidemiologica dell'influenza aviaria nell'Unione. In particolare, la decisione di esecuzione (UE) 2017/247 è stata modificata dalla decisione di esecuzione (UE) 2017/696 <sup>(5)</sup> al fine di stabilire norme concernenti la spedizione di pulcini di un giorno dalle zone elencate nell'allegato della decisione di esecuzione (UE) 2017/247. Tale modifica ha tenuto conto del fatto che i pulcini di un giorno presentano un rischio molto basso di diffusione dell'influenza aviaria ad alta patogenicità rispetto ad altri prodotti avicoli.
- (4) La decisione di esecuzione (UE) 2017/247 è stata inoltre successivamente modificata dalla decisione di esecuzione (UE) 2017/1841 <sup>(6)</sup> allo scopo di rafforzare le misure di lotta contro la malattia applicabili laddove si presenti un maggiore rischio di diffusione dell'influenza aviaria ad alta patogenicità. Di conseguenza, la decisione di esecuzione (UE) 2017/247 prevede ora l'istituzione a livello dell'Unione, a norma dell'articolo 16, paragrafo 4, della direttiva 2005/94/CE, di ulteriori zone di restrizione negli Stati membri interessati a seguito della comparsa

<sup>(1)</sup> GUL 395 del 30.12.1989, pag. 13.

<sup>(2)</sup> GUL 224 del 18.8.1990, pag. 29.

<sup>(3)</sup> Decisione di esecuzione (UE) 2017/247 della Commissione, del 9 febbraio 2017, relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri (GUL 36 dell'11.2.2017, pag. 62).

<sup>(4)</sup> Direttiva 2005/94/CE del Consiglio, del 20 dicembre 2005, relativa a misure comunitarie di lotta contro l'influenza aviaria e che abroga la direttiva 92/40/CEE (GUL 10 del 14.1.2006, pag. 16).

<sup>(5)</sup> Decisione di esecuzione (UE) 2017/696 della Commissione, dell'11 aprile 2017, che modifica la decisione di esecuzione (UE) 2017/247 relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri (GUL 101 del 13.4.2017, pag. 80).

<sup>(6)</sup> Decisione di esecuzione (UE) 2017/1841 della Commissione, del 10 ottobre 2017, che modifica la decisione di esecuzione (UE) 2017/247 relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri (GUL 261 dell'11.10.2017, pag. 26).

di uno o più focolai di influenza aviaria ad alta patogenicità, e dispone la durata delle misure da applicarsi in tali zone. La decisione di esecuzione (UE) 2017/247 stabilisce attualmente anche norme relative alla spedizione in altri Stati membri di pollame vivo, pulcini di un giorno e uova da cova dalle ulteriori zone di restrizione, nel rispetto di determinate condizioni.

- (5) Anche l'allegato della decisione di esecuzione (UE) 2017/247 è stato ripetutamente modificato, principalmente per tenere conto delle modifiche dei confini delle zone di protezione e sorveglianza istituite dagli Stati membri interessati a norma della direttiva 2005/94/CE.
- (6) L'allegato della decisione di esecuzione (UE) 2017/247 è stato da ultimo modificato dalla decisione di esecuzione (UE) 2018/510 <sup>(1)</sup> a seguito della notifica, da parte della Germania, della comparsa di un nuovo focolaio di influenza aviaria ad alta patogenicità del sottotipo H5N6 in un'azienda avicola situata in Frisia Settentrionale, nel *Land* Schleswig-Holstein di tale Stato membro. La Germania ha inoltre comunicato alla Commissione di aver debitamente adottato, a seguito della comparsa di tale focolaio, le misure necessarie prescritte dalla direttiva 2005/94/CE, tra cui l'istituzione di zone di protezione e sorveglianza intorno all'azienda avicola infetta.
- (7) Dalla data in cui è stata apportata l'ultima modifica alla decisione di esecuzione (UE) 2017/247 mediante la decisione di esecuzione (UE) 2018/510, la Bulgaria ha notificato alla Commissione la comparsa di un recente focolaio di influenza aviaria ad alta patogenicità del sottotipo H5N8 in un'azienda avicola nella regione di Yambol di tale Stato membro.
- (8) La Bulgaria ha inoltre comunicato alla Commissione di aver adottato, a seguito della comparsa di tale recente focolaio, le misure necessarie prescritte dalla direttiva 2005/94/CE, tra cui l'istituzione di zone di protezione e sorveglianza intorno all'azienda avicola infetta in tale Stato membro.
- (9) La Commissione ha esaminato tali misure in collaborazione con la Bulgaria e ha potuto accertare che i confini delle zone di protezione e sorveglianza istituite dall'autorità competente in tale Stato membro si trovano a una distanza sufficiente dall'azienda avicola in cui è stata confermata la comparsa del nuovo focolaio.
- (10) Al fine di prevenire inutili perturbazioni degli scambi all'interno dell'Unione ed evitare che paesi terzi impongano ostacoli ingiustificati agli scambi, è necessario descrivere rapidamente a livello dell'Unione, in collaborazione con la Bulgaria, le zone di protezione e sorveglianza istituite in tale Stato membro in conformità della direttiva 2005/94/CE a seguito della comparsa del recente focolaio di influenza aviaria ad alta patogenicità in tale Stato membro.
- (11) È pertanto opportuno aggiornare la decisione di esecuzione (UE) 2017/247 per tenere conto della nuova situazione epidemiologica relativa all'influenza aviaria ad alta patogenicità in Bulgaria. In particolare, le zone di protezione e sorveglianza recentemente istituite in Bulgaria, attualmente soggette a restrizioni a norma della direttiva 2005/94/CE, dovrebbero essere elencate nell'allegato della decisione di esecuzione (UE) 2017/247.
- (12) L'allegato della decisione di esecuzione (UE) 2017/247 dovrebbe pertanto essere modificato al fine di aggiornare la regionalizzazione a livello dell'Unione, per includere le zone di protezione e sorveglianza istituite in Bulgaria in conformità della direttiva 2005/94/CE a seguito della comparsa del recente focolaio di influenza aviaria ad alta patogenicità in tale Stato membro, e la durata delle restrizioni in esse applicabili.
- (13) È pertanto opportuno modificare di conseguenza la decisione di esecuzione (UE) 2017/247.
- (14) Le misure di cui alla presente decisione sono conformi al parere del comitato permanente per le piante, gli animali, gli alimenti e i mangimi,

HA ADOTTATO LA PRESENTE DECISIONE:

#### Articolo 1

L'allegato della decisione di esecuzione (UE) 2017/247 è modificato conformemente all'allegato della presente decisione.

<sup>(1)</sup> Decisione di esecuzione (UE) 2018/510 della Commissione, del 26 marzo 2018, che modifica l'allegato della decisione di esecuzione (UE) 2017/247 relativa a misure di protezione contro i focolai di influenza aviaria ad alta patogenicità in alcuni Stati membri (GU L 83 del 27.3.2018, pag. 16).

---

*Articolo 2*

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 10 aprile 2018

*Per la Commissione*  
Vytenis ANDRIUKAITIS  
*Membro della Commissione*

---

## ALLEGATO

L'allegato della decisione di esecuzione (UE) 2017/247 è così modificato:

1) nella parte A la voce relativa alla Bulgaria è sostituita dalla seguente:

«**Stato membro: Bulgaria**

Area comprendente	Termine ultimo di applicazione a norma dell'articolo 29, paragrafo 1, della direttiva 2005/94/CE
Regione di Yambol, comune di Straldzha	
Zimnitsa	26.4.2018»;

2) nella parte B la voce relativa alla Bulgaria è sostituita dalla seguente:

«**Stato membro: Bulgaria**

Area comprendente	Termine ultimo di applicazione a norma dell'articolo 31 della direttiva 2005/94/CE
<b>Regione di Yambol:</b>	
comune di Straldzha — Zimnitsa	dal 27.4.2018 al 6.5.2018
comune di Yambol — Yambol	6.5.2018».
comune di Straldzha — Straldzha — Vodenichene — Dzhinot	
comune di Tundzha — Mogila — Veselinovo — Kabile	
<b>Regione di Sliven:</b>	
comune di Sliven — Zhelyu Voivoda — Blatets — Dragodanovo — Gorno Aleksandrovo	







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



**Ufficio delle pubblicazioni dell'Unione europea**  
2985 Lussemburgo  
LUSSEMBURGO

**IT**