

REGOLAMENTO DI ESECUZIONE (UE) 2019/1583 DELLA COMMISSIONE**del 25 settembre 2019****che modifica il regolamento di esecuzione (UE) 2015/1998 che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, per quanto riguarda le misure di cibersicurezza****(Testo rilevante ai fini del SEE)**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 ⁽¹⁾, in particolare l'articolo 1 e l'articolo 4, paragrafo 3,

considerando quanto segue:

- (1) Uno dei principali obiettivi del regolamento (CE) n. 300/2008 è definire i criteri per un'interpretazione comune dell'annesso 17 (annesso sulla sicurezza) della Convenzione internazionale per l'aviazione civile ⁽²⁾, del 7 dicembre 1944, 10^a edizione, 2017, di cui tutti gli Stati membri dell'UE sono firmatari.
- (2) I mezzi per conseguire gli obiettivi sono: a) la definizione di regole e di norme fondamentali comuni in relazione alla sicurezza aerea; b) meccanismi di controllo della conformità.
- (3) Alla base della modifica della legislazione di esecuzione vi è l'intento di aiutare gli Stati membri a garantire il pieno rispetto della modifica più recente (modifica 16) dell'annesso 17 della Convenzione internazionale per l'aviazione civile, con cui sono state introdotte nuove norme ai capitoli 3.1.4, relativo all'organizzazione nazionale e all'autorità competente, e 4.9.1, concernente le misure preventive di cibersicurezza.
- (4) Recependo tali norme nella legislazione di esecuzione dell'UE riguardante la sicurezza aerea sarà fatto in modo che le autorità competenti stabiliscano e attuino procedure per la condivisione, ove opportuna, tempestiva e pratica delle informazioni pertinenti di ausilio ad altre autorità e agenzie nazionali, agli operatori aeroportuali, ai vettori aerei e ad altri soggetti interessati, di modo che possano eseguire efficaci valutazioni dei rischi per la sicurezza in relazione alle loro operazioni ed anche, fra l'altro, alla cibersicurezza e all'attuazione di misure volte a contrastare le minacce informatiche.
- (5) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ⁽³⁾ recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS), stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione al fine di migliorare il funzionamento del mercato interno. Le misure derivanti dalla direttiva NIS e dal presente regolamento dovrebbero essere coordinate a livello nazionale per evitare lacune e duplicazioni degli obblighi.
- (6) È pertanto opportuno modificare di conseguenza il regolamento di esecuzione (UE) 2015/1998 della Commissione ⁽⁴⁾.
- (7) Le misure di cui al presente regolamento sono conformi al parere del comitato per la sicurezza dell'aviazione civile istituito dall'articolo 19, paragrafo 1, del regolamento (CE) n. 300/2008,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

L'allegato del regolamento di esecuzione (UE) 2015/1998 è modificato conformemente all'allegato del presente regolamento.

⁽¹⁾ GUL 97 del 9.4.2008, pag. 72.⁽²⁾ <https://icao.int/publications/pages/doc7300.aspx>⁽³⁾ Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GUL 194 del 19.7.2016, pag. 1).⁽⁴⁾ Regolamento di esecuzione (UE) 2015/1998 della Commissione, del 5 novembre 2015, che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea (GUL 299 del 14.11.2015, pag. 1).

Articolo 2

Il presente regolamento entra in vigore il 31 dicembre 2020.

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

Fatto a Bruxelles, il 25 settembre 2019

Per la Commissione
Il presidente
Jean-Claude JUNCKER

ALLEGATO

L'allegato del regolamento di esecuzione (UE) 2015/1998 è così modificato:

1) è aggiunto il seguente punto 1.0.6:

«1.0.6. L'autorità competente deve stabilire e attuare procedure per la condivisione, ove opportuna, tempestiva e pratica delle informazioni pertinenti di ausilio ad altre autorità e agenzie nazionali, agli operatori aeroportuali, ai vettori aerei e ad altri soggetti interessati, di modo che possano eseguire efficaci valutazioni dei rischi per la sicurezza in relazione alle loro operazioni.»;

2) è aggiunto il seguente punto 1.7:

«1.7 INDIVIDUAZIONE DEI DATI E DEI SISTEMI DI TECNOLOGIA DELL'INFORMAZIONE E DELLA COMUNICAZIONE FONDAMENTALI PER L'AVIAZIONE CIVILE E LORO PROTEZIONE DALLE MINACCE INFORMATICHE

1.7.1. L'autorità competente deve fare in modo che gli operatori aeroportuali, i vettori aerei e gli altri soggetti definiti nel programma nazionale per la sicurezza dell'aviazione civile individuino e proteggano i dati e i sistemi fondamentali di tecnologia dell'informazione e della comunicazione da attacchi informatici che potrebbero pregiudicare la sicurezza dell'aviazione civile.

1.7.2. Operatori aeroportuali, vettori aerei ed altri soggetti devono individuare nel proprio programma di sicurezza, o in qualsiasi documento pertinente cui sia fatto riferimento nel programma di sicurezza, i dati e i sistemi fondamentali di tecnologia dell'informazione e della comunicazione di cui al punto 1.7.1.

Nel programma di sicurezza, ovvero nel documento pertinente eventualmente indicato nel programma di sicurezza, devono essere descritte in dettaglio le misure protettive predisposte nei confronti degli attacchi informatici, oltre alle misure per il riconoscimento di tali attacchi, come descritto al punto 1.7.1.

1.7.3. Le misure di protezione dettagliate di tali dati e sistemi dalle interferenze illecite devono essere individuate, elaborate e attuate in conformità a una valutazione del rischio effettuata dall'operatore aeroportuale, dal vettore aereo o dal soggetto in questione, a seconda dei casi.

1.7.4. Negli Stati membri in cui la competenza per le misure relative alle minacce informatiche spetta a un'autorità o a un'agenzia specifica, tale autorità o agenzia può essere designata come l'ente preposto al coordinamento e/o al controllo delle disposizioni concernenti la cibersicurezza di cui al presente regolamento.

1.7.5. Nel caso in cui determinati operatori aeroportuali, vettori aerei e altri soggetti definiti nel programma nazionale di sicurezza dell'aviazione civile soggiacciano ad obblighi di cibersicurezza a parte, derivanti da altre normative dell'UE o nazionali, l'autorità competente può stabilire che al posto delle prescrizioni del presente regolamento debbano essere rispettate le prescrizioni di tali altre normative dell'UE o nazionali. L'autorità competente è tenuta a coordinarsi con le altre autorità competenti al fine di stabilire regimi di controllo coordinati o compatibili.»;

3) il punto 11.1.2 è sostituito dal seguente:

«11.1.2. Il personale seguente deve aver superato un controllo rafforzato o standard dei precedenti personali:

- a) le persone selezionate per effettuare o far effettuare sotto la propria responsabilità controlli (screening), controlli dell'accesso o altri controlli di sicurezza in una zona diversa da un'area sterile;
- b) le persone che hanno accesso senza scorta alla merce e alla posta aerea, alla posta e al materiale del vettore aereo, alle provviste di bordo e alle forniture per l'aeroporto che sono stati sottoposti ai controlli di sicurezza prescritti;
- c) le persone che dispongono di diritti di amministratore o di accesso illimitato non controllato a dati e sistemi fondamentali di tecnologia dell'informazione e della comunicazione utilizzati per la sicurezza dell'aviazione civile, di cui al punto 1.7.1, in conformità al programma nazionale di sicurezza dell'aviazione civile, o che sono state altrimenti individuate nella valutazione dei rischi a norma del punto 1.7.3.

Salvo diversamente indicato nel presente regolamento, a stabilire se sia necessario effettuare un controllo rafforzato oppure standard dei precedenti personali deve essere l'autorità competente, conformemente alle norme nazionali applicabili.»;

4) è aggiunto il seguente punto 11.2.8:

«11.2.8. Addestramento delle persone con mansioni e responsabilità attinenti alle minacce informatiche

11.2.8.1. Le persone che attuano le misure di cui al punto 1.7.2 devono possedere le competenze e le attitudini necessarie ad eseguire in modo efficace i compiti loro assegnati e devono essere messe a conoscenza dei rischi informatici pertinenti limitatamente a quanto è necessario che sappiano in funzione del proprio incarico (principio della “necessità di conoscere”).

11.2.8.2. Le persone che hanno accesso a dati o sistemi devono ricevere un addestramento adeguato e specifico per il loro ruolo, commisurato alle loro mansioni e alle loro responsabilità, e devono essere sensibilizzate riguardo ai rischi qualora ciò sia reso necessario dalla funzione che rivestono. L'autorità competente, oppure l'autorità o l'agenzia di cui al punto 1.7.4, deve indicare o approvare i contenuti del corso.».
