REGOLAMENTO DELEGATO (UE) 2022/1645 DELLA COMMISSIONE

del 14 luglio 2022

recante modalità di applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le imprese disciplinate dai regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione e che modifica i regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio ([1]), in particolare l'articolo 19, paragrafo 1, lettera g), e l'articolo 39, paragrafo 1, lettera b),

considerando quanto segue:

(1) Conformemente ai requisiti essenziali di cui all'allegato II, punto 3.1, lettera b), del regolamento (UE) 2018/1139, le organizzazioni di progettazione e produzione devono realizzare e mantenere un sistema di gestione per gestire i rischi in materia di sicurezza.

(2) Inoltre, conformemente ai requisiti essenziali di cui all'allegato VII, punti 2.2.1 e 5.2, del regolamento (UE) 2018/1139, i gestori aeroportuali e le organizzazioni responsabili della fornitura di servizi di gestione del piazzale devono realizzare e mantenere un sistema di gestione per gestire i rischi in materia di sicurezza.

(3) I rischi in materia di sicurezza di cui ai considerando 1 e 2 possono derivare da varie fonti, tra cui difetti di progettazione e di manutenzione, aspetti relativi alle prestazioni umane, minacce ambientali e alla sicurezza delle informazioni. È opportuno pertanto che i sistemi di gestione realizzati dalle organizzazioni di cui ai considerando 1 e 2 tengano conto non solo dei rischi in materia di sicurezza derivanti da eventi casuali, ma anche dei rischi in materia di sicurezza derivanti da minacce alla sicurezza delle informazioni in cui le falle esistenti possono essere sfruttate da individui con l'intento di nuocere. Tali rischi per la sicurezza delle informazioni sono in costante aumento nell'ambiente dell'aviazione civile dal momento che gli attuali sistemi informativi stanno diventando sempre più interconnessi e sempre più bersaglio di attori malintenzionati.

(4) I rischi associati a tali sistemi informativi non si limitano a possibili attacchi al ciberspazio, ma comprendono anche minacce che possono influire sui processi e sulle procedure nonché sulle prestazioni umane.

(5) Un numero significativo di imprese utilizza già norme internazionali, come l'ISO 27001, al fine di affrontare la questione della sicurezza delle informazioni e dei dati digitali. Tali norme potrebbero non affrontare pienamente tutte le specificità dell'aviazione civile.

(6) È pertanto opportuno stabilire requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea.

(7) È essenziale che tali requisiti riguardino i diversi settori dell'aviazione e le relative interfacce, dal momento che l'aviazione è un sistema di sistemi altamente interconnesso. Essi dovrebbero pertanto applicarsi a tutte le imprese che sono già tenute a disporre un sistema di gestione conformemente alla vigente normativa dell'Unione in materia di sicurezza aerea.

(8) I requisiti di cui al presente regolamento dovrebbero essere applicati in modo coerente in tutti i settori dell'aviazione, generando nel contempo un impatto minimo sulla legislazione dell'Unione in materia di sicurezza aerea già applicabile a tali settori.

([1]) GU L 212 del 22.8.2018, pag. 1.