ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/1583

z dnia 25 września 2019 r.

zmieniające rozporządzenie wykonawcze (UE) 2015/1998 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego w odniesieniu do środków w zakresie cyberbezpieczeństwa

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 ([1]), w szczególności jego art. 1 i art. 4 ust. 3,

a także mając na uwadze, co następuje:

(1) Jednym z głównych celów rozporządzenia (WE) nr 300/2008 jest zapewnienie podstaw wspólnej wykładni Załącznika 17 (załącznika dotyczącego ochrony) do Konwencji o międzynarodowym lotnictwie cywilnym ([2]) z dnia 7 grudnia 1944 r., wyd. 10, 2017 r., której sygnatariuszami są wszystkie państwa członkowskie UE.

(2) Środkiem do osiągnięcia powyższych celów jest: a) ustanowienie wspólnych zasad i wspólnych podstawowych norm ochrony lotnictwa oraz b) mechanizmy monitorowania ich przestrzegania.

(3) Celem zmiany przepisów wykonawczych jest wspieranie państw członkowskich w zapewnianiu pełnej zgodności z najnowszą poprawką (poprawka 16) do Załącznika 17 do Konwencji o międzynarodowym lotnictwie cywilnym, w której wprowadzono nowe normy dotyczące organizacji krajowej i właściwego organu (rozdział 3.1.4) oraz środków zapobiegawczych w zakresie cyberbezpieczeństwa (rozdział 4.9.1).

(4) Dzięki transpozycji tych norm do obowiązujących w całej Unii przepisów wykonawczych dotyczących ochrony lotnictwa zapewni się ustanowienie i wdrożenie przez właściwe organy procedur wymiany istotnych informacji, w stosownych przypadkach i w sposób praktyczny i terminowy, w celu wspierania innych organów i agencji krajowych, operatorów portów lotniczych, przewoźników lotniczych i innych zainteresowanych podmiotów w procesie przeprowadzania efektywnej oceny ryzyka w zakresie ochrony w odniesieniu do wykonywanej przez nich działalności i w ten sposób wspieranie tych podmiotów w przeprowadzaniu skutecznej oceny ryzyka w zakresie ochrony, m.in. w odniesieniu do cyberbezpieczeństwa, i we wdrażaniu środków eliminowania zagrożeń dla cyberbezpieczeństwa.

(5) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 ([3]) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji) ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii w celu poprawy funkcjonowania rynku wewnętrznego. Środki wynikające z dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz z niniejszego rozporządzenia powinny być koordynowane na poziomie krajowym, aby uniknąć luk i powielania obowiązków.

(6) Należy zatem odpowiednio zmienić rozporządzenie wykonawcze Komisji (UE) 2015/1998 ([4]).

(7) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Ochrony Lotnictwa Cywilnego utworzonego na podstawie art. 19 ust. 1 rozporządzenia (WE) nr 300/2008,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W załączniku do rozporządzenia wykonawczego (UE) 2015/1998 wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

([1]) Dz.U. L 97 z 9.4.2008, s. 72.
([2]) https://icao.int/publications/pages/doc7300.aspx
([3]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).
([4]) Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (Dz.U. L 299 z 14.11.2015, s. 1).

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie z dniem 31 grudnia 2020 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 25 września 2019 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK

W załączniku do rozporządzenia wykonawczego (UE) 2015/1998 wprowadza się następujące zmiany:

1) dodaje się punkt 1.0.6 w brzmieniu:

„1.0.6. Właściwy organ ustanawia i wdraża procedury wymiany istotnych informacji, w stosownych przypadkach i w sposób praktyczny i terminowy, w celu wspierania innych organów i agencji krajowych, operatorów portów lotniczych, przewoźników lotniczych i innych zainteresowanych podmiotów w procesie przeprowadzania skutecznej oceny ryzyka w zakresie ochrony w odniesieniu do wykonywanych przez nich rodzajów działalności.";

2) dodaje się pkt 1.7 w brzmieniu:

„1.7. IDENTYFIKACJA SYSTEMÓW TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH I DANYCH KRYTYCZNYCH DLA LOTNICTWA CYWILNEGO ORAZ ICH OCHRONA PRZED ZAGROŻENIAMI DLA CYBERBEZPIECZEŃSTWA

1.7.1. Właściwy organ zapewnia, aby określeni w krajowym programie ochrony lotnictwa cywilnego operatorzy portów lotniczych, przewoźnicy lotniczy i podmioty identyfikowali swoje krytyczne systemy technologii informacyjno-komunikacyjnych i dane i chronili je przed cyberatakami, które mogłyby wpłynąć na bezpieczeństwo lotnictwa cywilnego.

1.7.2. Operatorzy portów lotniczych, przewoźnicy lotniczy i podmioty określają w swoim programie ochrony lub w innym odpowiednim dokumencie wymienionym w programie ochrony, krytyczne systemy technologii informacyjno-komunikacyjnych i dane zgodnie z pkt 1.7.1.

W programie ochrony lub w innym odpowiednim dokumencie, o którym mowa w programie ochrony, określa się szczegółowo środki mające na celu zapewnienie ochrony przed cyberatakami, które mogłyby wpłynąć na bezpieczeństwo lotnictwa cywilnego, wykrywania ich i reagowania na nie, zgodnie z pkt 1.7.1.

1.7.3. Szczegółowe środki mające na celu ochronę takich systemów i danych przed bezprawną ingerencją określa się, opracowuje i wdraża zgodnie z oceną ryzyka przeprowadzoną odpowiednio przez operatora portu lotniczego, przewoźnika lotniczego lub inny podmiot.

1.7.4. Jeżeli w obrębie jednego państwa członkowskiego w zakresie środków związanych z zagrożeniami dla cyberbezpieczeństwa wyznaczony jest organ lub agencja, ten organ lub agencja mogą zostać desygnowane jako odpowiednie do celów koordynacji lub monitorowania przepisów dotyczących cyberbezpieczeństwa określonych w niniejszym rozporządzeniu.

1.7.5. Jeżeli określeni w krajowym programie ochrony lotnictwa cywilnego operatorzy portów lotniczych, przewoźnicy lotniczy i podmioty podlegają odrębnym wymogom w zakresie cyberbezpieczeństwa wynikającym z innych przepisów unijnych lub krajowych, właściwy organ może zastąpić zgodność z wymogami niniejszego rozporządzenia zgodnością z elementami zawartymi w innych przepisach unijnych lub krajowych. Właściwy organ koordynuje swoje działania z wszelkimi innymi odpowiednimi wyznaczonymi organami w celu zapewnienia skoordynowanych lub kompatybilnych systemów nadzoru.";

3) pkt 11.1.2 otrzymuje brzmienie:

„11.1.2. Następujący personel musi przejść rozszerzone lub standardowe sprawdzenie przeszłości z wynikiem pozytywnym:

a) Osoby rekrutowane w celu przeprowadzania kontroli bezpieczeństwa, kontroli dostępu lub stosowania innych środków kontroli w zakresie ochrony w miejscach innych niż strefa zastrzeżona lotniska, lub sprawowania odpowiedzialności za przeprowadzanie tych kontroli;

b) Osoby mające dostęp bez eskorty do ładunku lotniczego i poczty lotniczej, poczty przewoźnika lotniczego i materiałów przewoźnika lotniczego, zaopatrzenia pokładowego i zaopatrzenia portu lotniczego, do których zastosowano wymagane środki kontroli w zakresie ochrony;

c) Osoby mające uprawnienia administratora lub nieograniczony dostęp bez nadzoru do krytycznych systemów technologii informacyjno-komunikacyjnych i danych, wykorzystywanych do celów ochrony lotnictwa cywilnego zgodnie z pkt 1.7.1, zgodnie z krajowym programem ochrony lotnictwa lub które zostały w inny sposób określone w ocenie ryzyka zgodnie z pkt 1.7.3.

O tym, czy należy przeprowadzać rozszerzone czy standardowe sprawdzenie przeszłości, decyduje właściwy organ, działając zgodnie z mającymi zastosowanie przepisami krajowymi, chyba że w niniejszym rozporządzeniu określono inaczej.";

4) dodaje się punkt 11.2.8 w brzmieniu:

„11.2.8. Szkolenie osób pełniących role lub wykonujących obowiązki związane z zagrożeniami dla cyberbezpieczeństwa

11.2.8.1. Osoby wdrażające środki ustanowione w pkt 1.7.2 posiadają kwalifikacje i umiejętności niezbędne do skutecznego wykonywania wyznaczonych zadań. Są one informowane o istotnych przypadkach zagrożeń dla cyberbezpieczeństwa zgodnie z zasadą ograniczonego dostępu.

11.2.8.2. Osoby mające dostęp do danych lub systemów przechodzą odpowiednie i specjalistyczne szkolenie zawodowe, współmierne do swojej roli i obowiązków, uwzględniające informacje o istotnych zagrożeniach, jeżeli wymaga tego zajmowane stanowisko pracy. Właściwy organ lub organ lub agencja określone w pkt 1.7.4 określają lub zatwierdzają treść kursu.”.