II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2023/203

z dnia 27 października 2022 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w kwestii wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373 i (UE) 2021/664 oraz właściwych organów objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012, (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373, (UE) nr 139/2014 i (UE) 2021/664 oraz zmieniające rozporządzenia Komisji (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 ([1]), w szczególności jego art. 17 ust. 1 lit. b), art. 27 ust. 1 lit. a), art. 31 ust. 1 lit. b), art. 43 ust. 1 lit. b), art. 53 ust. 1 lit. a) i art. 62 ust. 15 lit. c),

a także mając na uwadze, co następuje:

(1) Zgodnie z zasadniczymi wymogami określonymi w pkt 3.1 lit. b) załącznika II do rozporządzenia (UE) 2018/1139 organizacje zarządzania ciągłą zdatnością do lotu i organizacje obsługi technicznej muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

(2) Ponadto zgodnie z zasadniczymi wymogami określonymi w pkt 3.3 lit. b) i pkt 5 lit. b) załącznika IV do rozporządzenia (UE) 2018/1139 organizacje szkolące pilotów, organizacje szkolące personel pokładowy, centra medycyny lotniczej dla załóg oraz operatorzy szkoleniowych urządzeń symulacji lotu muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

(3) Co więcej, zgodnie z zasadniczymi wymogami określonymi w pkt 8.1 lit. c) załącznika V do rozporządzenia (UE) 2018/1139 przewoźnicy lotniczy muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

(4) Ponadto zgodnie z zasadniczymi wymogami określonymi w pkt 5.1 lit. c) i pkt 5.4 lit. b) załącznika VIII do rozporządzenia (UE) 2018/1139 instytucje zapewniające zarządzanie ruchem lotniczym i instytucje zapewniające służby żeglugi powietrznej, instytucje świadczące usługi U-space i wyłączne instytucje świadczące centralne usługi informacyjne, a także organizacje szkoleniowe i centra medycyny lotniczej dla kontrolerów ruchu lotniczego muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

([1]) Dz.U. L 212 z 22.8.2018, s. 1.

(5) Odnośne ryzyko dotyczące bezpieczeństwa może wynikać z różnych źródeł, takich jak wady projektowe, nieprawidłowe utrzymanie, aspekty wydolności ludzkiej, zagrożenia środowiskowe i zagrożenia dla bezpieczeństwa informacji. W systemach zarządzania wdrożonych przez Agencję Unii Europejskiej ds. Bezpieczeństwa Lotniczego („Agencja"), właściwe organy krajowe oraz organizacje, o których mowa w motywach powyżej, należy zatem uwzględnić nie tylko ryzyko dla bezpieczeństwa wynikające ze zdarzeń losowych, ale również ryzyko dla bezpieczeństwa wynikające z zagrożeń dla bezpieczeństwa informacji, jeżeli występujące wady mogą zostać wykorzystane przez osoby fizyczne w złym zamiarze. Tego typu ryzyko związane z bezpieczeństwem informacji stale wzrasta w środowisku lotnictwa cywilnego wraz z coraz większym powiązaniem obecnie funkcjonujących systemów informatycznych, które coraz częściej stają się celem ataków dokonywanych przez osoby działające w złym zamiarze.

(6) Ryzyko związane z tymi systemami informatycznymi nie ogranicza się do ewentualnych ataków w cyberprzestrzeni, ale obejmuje również zagrożenia, które mogą wpływać na procesy i procedury, a także wydolność ludzką.

(7) Aby zapewnić bezpieczeństwo informacji i danych cyfrowych, wiele organizacji już teraz stosuje normy międzynarodowe, takie jak ISO 27001. Normy te mogą nie obejmować wszystkich aspektów lotnictwa cywilnego. Należy zatem określić wymagania dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze.

(8) Ważne jest, aby takie wymagania obejmowały wszystkie dziedziny lotnictwa i ich wzajemne relacje, ponieważ lotnictwo stanowi wysoce powiązany system systemów. Wymagania te muszą zatem mieć zastosowanie do wszystkich organizacji i właściwych organów objętych rozporządzeniami Komisji (UE) nr 748/2012 ([2]), (UE) nr 1321/2014 ([3]), (UE) nr 965/2012 ([4]), (UE) nr 1178/2011 ([5]), (UE) 2015/340 ([6]), (UE) nr 139/2014 ([7]) i rozporządzeniem wykonawczym Komisji (UE) 2021/664 ([8]), a także do tych, które już teraz są zobowiązane do posiadania systemu zarządzania zgodnie z obowiązującymi unijnymi przepisami dotyczącymi bezpieczeństwa lotniczego. Niektóre organizacje należy jednak wyłączyć z zakresu stosowania niniejszego rozporządzenia w celu zapewnienia odpowiedniej proporcjonalności do niższego ryzyka związanego z bezpieczeństwem informacji, na jakie narażają one system lotnictwa.

(9) Wymagania określone w niniejszym rozporządzeniu powinny zapewnić konsekwentne wdrażanie we wszystkich dziedzinach lotnictwa, a jednocześnie ich stosowanie powinno mieć jak najmniejszy wpływ na unijne przepisy dotyczące bezpieczeństwa lotniczego mające już zastosowanie do tych dziedzin.

([2]) Rozporządzenie Komisji (UE) nr 748/2012 z dnia 3 sierpnia 2012 r. ustanawiające przepisy wykonawcze dotyczące certyfikacji statków powietrznych i związanych z nimi wyrobów, części i akcesoriów w zakresie zdatności do lotu i ochrony środowiska oraz dotyczące certyfikacji organizacji projektujących i produkujących (Dz. U. L 224 z 21.8.2012, s. 1).

([3]) Rozporządzenie Komisji (UE) nr 1321/2014 z dnia 26 listopada 2014 r. w sprawie ciągłej zdatności do lotu statków powietrznych oraz wyrobów lotniczych, części i wyposażenia, a także w sprawie zatwierdzeń udzielanych organizacjom i personelowi zaangażowanym w takie zadania (Przekształcenie) (Dz.U. L 362 z 17.12.2014, s. 1).

([4]) Rozporządzenie Komisji (UE) nr 965/2012 z dnia 5 października 2012 r. ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do operacji lotniczych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008 (Dz.U. L 296 z 25.10.2012, s. 1).

([5]) Rozporządzenie Komisji (UE) nr 1178/2011 z dnia 3 listopada 2011 r. ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do załóg w lotnictwie cywilnym zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008 (Dz.U. L 311 z 25.11.2011, s. 1).

([6]) Rozporządzenie Komisji (UE) 2015/340 z dnia 20 lutego 2015 r. ustanawiające wymagania techniczne i procedury administracyjne dotyczące licencji i certyfikatów kontrolerów ruchu lotniczego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008, zmieniające rozporządzenie wykonawcze Komisji (UE) nr 923/2012 i uchylające rozporządzenie Komisji (UE) nr 805/2011 (Dz.U. L 63 z 6.3.2015, s. 1).

([7]) Rozporządzenie Komisji (UE) nr 139/2014 z dnia 12 lutego 2014 r. ustanawiające wymagania oraz procedury administracyjne dotyczące lotnisk zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008 (Dz.U. L 44 z 14.2.2014, s. 1).

([8]) Rozporządzenie wykonawcze Komisji (UE) 2021/664 z dnia 22 kwietnia 2021 r. w sprawie ram regulacyjnych dotyczących U-space (Dz.U. L 139 z 23.4.2021, s. 161).

(10) Wymagania określone w niniejszym rozporządzeniu powinny pozostawać bez uszczerbku dla wymogów w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa określonych w pkt 1.7 załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1998 ([9]) i w art. 14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([10]).

(11) Wymogi bezpieczeństwa określone w art. 33–43 tytułu V „Bezpieczeństwo programu" rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/696 ([11]) uznaje się za równoważne wymogom określonym w niniejszym rozporządzeniu, z wyjątkiem pkt IS.I.OR.230 załącznika II do niniejszego rozporządzenia, którego należy przestrzegać.

(12) W celu zagwarantowania pewności prawa należy uznać, że interpretacja terminu „bezpieczeństwo informacji" zdefiniowanego w niniejszym rozporządzeniu, odzwierciedlająca jego powszechne stosowanie w lotnictwie cywilnym na świecie, jest zgodna z interpretacją terminu „bezpieczeństwo sieci i systemów informatycznych" zdefiniowanego w art. 4 pkt 2 dyrektywy (UE) 2016/1148. Definicji terminu „bezpieczeństwo informacji" stosowanej do celów niniejszego rozporządzenia nie należy interpretować jako definicji rozbieżnej z definicją terminu „bezpieczeństwo sieci i systemów informatycznych" określoną w dyrektywie (UE) 2016/1148.

(13) Aby uniknąć powielania wymogów prawnych, jeżeli organizacje objęte zakresem niniejszego rozporządzenia podlegają już wymogom w zakresie bezpieczeństwa wynikającym z aktów Unii, o których mowa w motywach 10 i 11, i wywierającym taki sam skutek jak przepisy określone w niniejszym rozporządzeniu, zgodność z takimi wymogami w zakresie bezpieczeństwa należy uznać za tożsamą ze zgodnością z wymogami określonymi w niniejszym rozporządzeniu.

(14) Organizacje objęte zakresem stosowania niniejszego rozporządzenia, które już podlegają wymogom w zakresie bezpieczeństwa wynikającym z rozporządzenia wykonawczego (UE) 2015/1998 lub rozporządzenia (UE) 2021/696 bądź obydwu tych rozporządzeń, powinny również przestrzegać wymogów określonych w załączniku II (część IS.I.OR.230 „System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji") do niniejszego rozporządzenia, ponieważ żadne z tych rozporządzeń nie zawiera przepisów dotyczących zewnętrznego zgłaszania incydentów związanych z bezpieczeństwem informacji.

(15) W celu zapewnienia kompletności należy zmienić rozporządzenia (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze (UE) 2017/373 ([12]) i (UE) 2021/664, aby wprowadzić wymogi dotyczące systemu zarządzania bezpieczeństwem informacji przewidziane w niniejszym rozporządzeniu wraz z określonymi w nim systemami zarządzania oraz aby określić wymogi dla właściwych organów w zakresie nadzoru nad organizacjami wdrażającymi wspomniane wymogi dotyczące zarządzania bezpieczeństwem informacji.

(16) Aby organizacje miały wystarczająco dużo czasu na zapewnienie zgodności z nowymi przepisami i procedurami, niniejsze rozporządzenie stosuje się po upływie 3 lat od daty jego wejścia w życie, z wyjątkiem instytucji zapewniającej służby żeglugi powietrznej w ramach europejskiego systemu wspomagania satelitarnego (EGNOS) zdefiniowanej w rozporządzeniu wykonawczym (UE) 2017/373, w odniesieniu do której w związku z trwającą akredytacją bezpieczeństwa systemu i usług EGNOS zgodnie z rozporządzeniem (UE) 2021/696 niniejsze rozporządzenie powinno mieć zastosowanie od 1 stycznia 2026 r.

(17) Wymagania określone w niniejszym rozporządzeniu opierają się na opinii nr 03/2021 ([13]) wydanej przez Agencję zgodnie z art. 75 ust. 2 lit. b) i c) oraz art. 76 ust. 1 rozporządzenia (UE) 2018/1139.

([9]) 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).

([10]) 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).

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/696 z dnia 28 kwietnia 2021 r. ustanawiające Unijny program kosmiczny i Agencję Unii Europejskiej ds. Programu Kosmicznego oraz uchylające rozporządzenia (UE) nr 912/2010, (UE) nr 1285/2013 i (UE) nr 377/2014 oraz decyzję nr 541/2014/UE (Dz.U. L 170 z 12.5.2021, s. 69).

([12]) Rozporządzenie wykonawcze Komisji (UE) 2017/373 z dnia 1 marca 2017 r. ustanawiające wspólne wymogi dotyczące instytucji zapewniających zarządzanie ruchem lotniczym/służby żeglugi powietrznej i inne funkcje sieciowe zarządzania ruchem lotniczym oraz nadzoru nad nimi, uchylające rozporządzenie (WE) nr 482/2008, rozporządzenia wykonawcze (UE) nr 1034/2011, (UE) nr 1035/2011 i (UE) 2016/1377 oraz zmieniające rozporządzenie (UE) nr 677/2011 (Dz.U. L 62 z 8.3.2017, s. 1).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) Wymagania określone w niniejszym rozporządzeniu są zgodne z opinią komitetu ds. stosowania wspólnych zasad bezpieczeństwa w dziedzinie lotnictwa cywilnego ustanowionego na mocy art. 127 rozporządzenia (UE) 2018/1139,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się wymagania, które muszą spełnić organizacje i właściwe organy w celu:

a) określenia ryzyka związanego z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, co może wpływać na systemy technologii informacyjno-komunikacyjnych i dane wykorzystywane do celów lotnictwa cywilnego;

b) wykrywania zdarzeń związanych z bezpieczeństwem informacji i identyfikacji zdarzeń, które uznaje się za incydenty związane z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze;

c) reagowania na takie incydenty związane z bezpieczeństwem informacji i przywracania sytuacji sprzed takich incydentów.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do następujących organizacji:

a) organizacji obsługi technicznej podlegających sekcji A załącznika II (część 145) do rozporządzenia (UE) nr 1321/2014, z wyjątkiem organizacji zaangażowanych wyłącznie w obsługę techniczną statków powietrznych zgodnie z załącznikiem Vb (część ML) do rozporządzenia (UE) nr 1321/2014;

b) organizacji zarządzania ciągłą zdatnością do lotu (CAMO) podlegających sekcji A załącznika Vc (część CAMO) do rozporządzenia (UE) nr 1321/2014, z wyjątkiem organizacji zaangażowanych wyłącznie w zarządzanie ciągłą zdatnością do lotu statków powietrznych zgodnie z załącznikiem Vb (część ML) do rozporządzenia (UE) nr 1321/2014;

c) przewoźników lotniczych podlegających przepisom załącznika III (część ORO) do rozporządzenia (UE) nr 965/2012, z wyjątkiem przewoźników zaangażowanych wyłącznie w eksploatację któregokolwiek z poniższych urządzeń:

(i) statków powietrznych ELA2 zdefiniowanych w art. 1 ust. 2 lit. j) rozporządzenia (UE) nr 748/2012;

(ii) jednosilnikowych samolotów z napędem śmigłowym o maksymalnej operacyjnej konfiguracji miejsc pasażerskich wynoszącej nie więcej niż pięć, które nie są sklasyfikowane jako złożone statki powietrzne z napędem silnikowym, podczas startu i lądowania na tym samym lotnisku lub w tym samym miejscu operacji lotniczej oraz wykonywania lotu według przepisów wykonywania lotu z widocznością (VFR) w dzień;

(iii) jednosilnikowych śmigłowców o maksymalnej operacyjnej konfiguracji miejsc pasażerskich wynoszącej nie więcej niż pięć, które nie są sklasyfikowane jako złożone statki powietrzne z napędem silnikowym, podczas startu i lądowania na tym samym lotnisku lub w tym samym miejscu operacji lotniczej oraz wykonywania lotu VFR w dzień;

d) zatwierdzonych organizacji szkolenia (ATO) podlegających załącznikowi VII (część ORA) do rozporządzenia (UE) nr 1178/2011, z wyjątkiem organizacji, które zajmują się wyłącznie szkoleniem związanym ze statkami powietrznymi ELA2 zdefiniowanymi w art. 1 ust. 2 lit. j) rozporządzenia (UE) nr 748/2012 lub wyłącznie szkoleniem teoretycznym;

e) centrów medycyny lotniczej dla załóg podlegających załącznikowi VII (część ORA) do rozporządzenia (UE) nr 1178/2011;

f) operatorów szkoleniowych urządzeń symulacji lotu (FSTD) podlegających załącznikowi VII (część ORA) do rozporządzenia (UE) nr 1178/2011, z wyjątkiem operatorów, którzy zajmują się wyłącznie eksploatacją FSTD do statków powietrznych ELA2 zdefiniowanych w art. 1 ust. 2 lit. j) rozporządzenia (UE) nr 748/2012;

g) organizacji szkolących kontrolerów ruchu lotniczego (ATCO TO) i centrów medycyny lotniczej dla kontrolerów ruchu lotniczego podlegających załącznikowi III (część ATCO.OR) do rozporządzenia (UE) 2015/340;

h) organizacji podlegających załącznikowi III (część ATM/ANS.OR) do rozporządzenia wykonawczego (UE) 2017/373, z wyjątkiem następujących instytucji:

(i) instytucji zapewniających służby żeglugi powietrznej posiadających certyfikat o ograniczonym zakresie zgodnie z pkt ATM/ANS.OR.A.010 tego załącznika;

(ii) instytucji zapewniających służby informacji powietrznej składających deklaracje o swojej działalności zgodnie z pkt ATM/ANS.OR.A.015 tego załącznika;

i) instytucji świadczących usługi U-space i wyłącznych instytucji świadczących centralne usługi informacyjne podlegających rozporządzeniu wykonawczemu (UE) 2021/664.

2. Niniejsze rozporządzenie ma zastosowanie do właściwych organów, w tym do Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego („Agencja"), o których mowa w art. 6 niniejszego rozporządzenia oraz w art. 5 rozporządzenia delegowanego Komisji (UE) 2022/1645 ([14]).

3. Niniejsze rozporządzenie ma również zastosowanie do właściwego organu odpowiedzialnego za wydawanie, przedłużanie, zmienianie, zawieszanie lub cofanie licencji na obsługę techniczną statków powietrznych zgodnie z załącznikiem III (część 66) do rozporządzenia (UE) nr 1321/2014.

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla wymogów w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa określonych w pkt 1.7 załącznika do rozporządzenia wykonawczego (UE) 2015/1998 i w art. 14 dyrektywy (UE) 2016/1148.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „bezpieczeństwo informacji" oznacza zachowanie poufności, integralności, autentyczności i dostępności sieci i systemów informatycznych;

2) „zdarzenie związane z bezpieczeństwem informacji" oznacza stwierdzone wystąpienie stanu systemu, usługi lub sieci wskazujące na możliwe naruszenie polityki bezpieczeństwa informacji lub niepowodzenie kontroli bezpieczeństwa informacji bądź nieznaną wcześniej sytuację, która może mieć znaczenie dla bezpieczeństwa informacji;

3) „incydent" oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych, zgodnie z definicją zawartą w art. 4 pkt 7 dyrektywy (UE) 2016/1148;

4) „ryzyko związane z bezpieczeństwem informacji" oznacza ryzyko dla operacji organizacyjnych lotnictwa cywilnego, zasobów, osób fizycznych i innych organizacji wynikające z możliwości wystąpienia zdarzenia związanego z bezpieczeństwem informacji. Ryzyko związane z bezpieczeństwem informacji wiąże się z możliwością wykorzystania podatności zasobów informacyjnych lub grupy zasobów informacyjnych na zagrożenia;

([14]) Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014 (Dz.U. L 248 z 26.9.2022, s. 18).

5) „zagrożenie" oznacza potencjalne naruszenie bezpieczeństwa informacji, które występuje w przypadku zaistnienia podmiotu, okoliczności, działania lub zdarzenia, które mogą spowodować szkodę;

6) „podatność" oznacza wadę lub słabość składnika aktywów lub systemu, procedur, projektu, wdrożenia lub środków bezpieczeństwa informacji, i które mogą zostać wykorzystane i prowadzić do naruszenia lub pogwałcenia strategii bezpieczeństwa informacji.

Artykuł 4

Wymogi dotyczące organizacji i właściwych organów

1. Organizacje, o których mowa w art. 2 ust. 1, muszą spełniać wymogi określone w załączniku II (część IS.I.OR) do niniejszego rozporządzenia.

2. Właściwe organy, o których mowa w art. 2 ust. 2 i 3, muszą spełniać wymogi określone w załączniku I (część IS.I. AR) do niniejszego rozporządzenia.

Artykuł 5

Wymogi wynikające z innych przepisów unijnych

1. Jeżeli organizacja, o której mowa w art. 2 ust. 1, przestrzega wymogów w zakresie bezpieczeństwa określonych zgodnie z art. 14 dyrektywy (UE) 2016/1148 równoważnych wymogom określonym w niniejszym rozporządzeniu, przestrzeganie tych wymogów uznaje się za tożsame z przestrzeganiem wymogów określonych w niniejszym rozporządzeniu.

2. Jeżeli organizacja, o której mowa w art. 2 ust. 1, jest operatorem lub podmiotem, o którym mowa w krajowych programach ochrony lotnictwa cywilnego państw członkowskich określonych zgodnie z art. 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 ([15]), wymogi w zakresie cyberbezpieczeństwa zawarte w pkt 1.7 załącznika do rozporządzenia wykonawczego (UE) 2015/1998 uznaje się za równoważne wymogom określonym w niniejszym rozporządzeniu, z wyjątkiem pkt IS.I.OR.230 załącznika II do niniejszego rozporządzenia, którego należy przestrzegać, zgodnie z jego treścią.

3. Jeżeli organizacja, o której mowa w art. 2 ust. 1, jest instytucją zapewniającą służby żeglugi powietrznej w ramach europejskiego systemu wspomagania satelitarnego (EGNOS), o której mowa w rozporządzeniu (UE) 2021/696, wymogi w zakresie bezpieczeństwa zawarte w art. 33–43 tytułu V tego rozporządzenia uznaje się za równoważne wymogom określonym w niniejszym rozporządzeniu, z wyjątkiem pkt IS.I.OR.230 załącznika II do niniejszego rozporządzenia, którego należy przestrzegać, zgodnie z jego treścią.

4. Komisja, po konsultacji z Agencją i grupą współpracy, o której mowa w art. 11 dyrektywy (UE) 2016/1148, może wydać wytyczne dotyczące oceny równoważności wymogów określonych w niniejszym rozporządzeniu i w dyrektywie (UE) 2016/1148.

Artykuł 6

Właściwy organ

1. Bez uszczerbku dla zadań powierzonych Radzie ds. Akredytacji Bezpieczeństwa (SAB), o której mowa w art. 36 rozporządzenia (UE) 2021/696, organem odpowiedzialnym za poświadczanie i nadzorowanie zgodności z niniejszym rozporządzeniem jest:

a) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. a), właściwy organ wyznaczony zgodnie z załącznikiem II (część 145) do rozporządzenia (UE) nr 1321/2014;

b) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. b), właściwy organ wyznaczony zgodnie z załącznikiem Vc (część CAMO) do rozporządzenia (UE) nr 1321/2014;

([15]) 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 (Dz.U. L 97 z 9.4.2008, s. 72).

c) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. c), właściwy organ wyznaczony zgodnie z załącznikiem III (część ORO) do rozporządzenia (UE) nr 965/2012;

d) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. d)–f), właściwy organ wyznaczony zgodnie z załącznikiem VII (część ORA) do rozporządzenia (UE) nr 1178/2011;

e) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. g), właściwy organ wyznaczony zgodnie z art. 6 ust. 2 rozporządzenia (UE) 2015/340;

f) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. h), właściwy organ wyznaczony zgodnie z art. 4 ust. 1 rozporządzenia wykonawczego (UE) 2017/373;

g) w odniesieniu do organizacji, o których mowa w art. 2 ust. 1 lit. i), właściwy organ wyznaczony, odpowiednio, zgodnie z art. 14 ust. 1 lub art. 14 ust. 2 rozporządzenia wykonawczego (UE) 2021/664.

2. Państwa członkowskie mogą do celów niniejszego rozporządzenia wyznaczyć niezależny i autonomiczny podmiot, który będzie pełnił przypisane mu role i obowiązki właściwych organów, o których mowa w ust. 1. W takim przypadku ustanawia się środki koordynacji między tym podmiotem a właściwymi organami, o których mowa w ust. 1, w celu zapewnienia skutecznego nadzoru w zakresie wszystkich wymagań, które ma spełnić dana organizacja.

3. Agencja współpracuje, zachowując pełną zgodność z obowiązującymi przepisami dotyczącymi tajemnicy, ochrony danych osobowych i ochrony informacji niejawnych, z Agencją Unii Europejskiej ds. Programu Kosmicznego (EUSPA) oraz z Radą ds. Akredytacji Bezpieczeństwa, o której mowa w art. 36 rozporządzenia (UE) 2021/696, w celu zapewnienia skutecznego nadzoru nad wymogami mającymi zastosowanie do instytucji zapewniającej służby żeglugi powietrznej w ramach EGNOS.

Artykuł 7

Przedkładanie odpowiednich informacji właściwym organom ds. bezpieczeństwa sieci i systemów informatycznych

Właściwe organy na podstawie niniejszego rozporządzenia bez zbędnej zwłoki informują pojedynczy punkt kontaktowy wyznaczony zgodnie z art. 8 dyrektywy (UE) 2016/1148 o wszelkich istotnych informacjach zawartych w powiadomieniach złożonych zgodnie z pkt IS.I.OR.230 załącznika II do niniejszego rozporządzenia oraz pkt IS.D.OR.230 załącznika I do rozporządzenia delegowanego 2022/1645 przez operatorów usług kluczowych zidentyfikowanych zgodnie z art. 5 dyrektywy (UE) 2016/1148.

Artykuł 8

Zmiana rozporządzenia (UE) nr 1178/2011

W załącznikach VI (część ARA) i VII (część ORA) do rozporządzenia (UE) nr 1178/2011 wprowadza się zmiany zgodnie z załącznikiem III do niniejszego rozporządzenia.

Artykuł 9

Zmiana rozporządzenia (UE) nr 748/2012

W załączniku I (część 21) do rozporządzenia (UE) nr 748/2012 wprowadza się zmiany zgodnie z załącznikiem IV do niniejszego rozporządzenia.

Artykuł 10

Zmiana rozporządzenia (UE) nr 965/2012

W załącznikach II (część ARO) i III (część ORO) do rozporządzenia (UE) nr 965/2012 wprowadza się zmiany zgodnie z załącznikiem V do niniejszego rozporządzenia.

Artykuł 11

Zmiana rozporządzenia (UE) nr 139/2014

W załączniku II (część ADR.AR) do rozporządzenia (UE) nr 139/2014 wprowadza się zmiany zgodnie z załącznikiem VI do niniejszego rozporządzenia.

Artykuł 12

Zmiana rozporządzenia (UE) nr 1321/2014

W załącznikach II (część 145), III (część 66) i Vc (część CAMO) do rozporządzenia (UE) nr 1321/2014 wprowadza się zmiany zgodnie z załącznikiem VII do niniejszego rozporządzenia.

Artykuł 13

Zmiana rozporządzenia (UE) 2015/340

W załącznikach II (część ATCO.AR) i III (część ATCO.OR) do rozporządzenia (UE) 2015/340 wprowadza się zmiany zgodnie z załącznikiem VIII do niniejszego rozporządzenia.

Artykuł 14

Zmiana rozporządzenia wykonawczego (UE) 2017/373

W załącznikach II (część ATM/ANS.AR) i III (część ATM/ANS.OR) do rozporządzenia wykonawczego (UE) 2017/373 wprowadza się zmiany zgodnie z załącznikiem IX do niniejszego rozporządzenia.

Artykuł 15

Zmiana rozporządzenia wykonawczego (UE) 2021/664

W rozporządzeniu wykonawczym (UE) 2021/664 wprowadza się następujące zmiany:

1) art. 15 ust. 1 lit. f) otrzymuje brzmienie:

„f) wdrożyły i utrzymują system zarządzania ochroną zgodnie z pkt ATM/ANS.OR.D.010 w podczęści D załącznika III do rozporządzenia wykonawczego (UE) 2017/373 oraz system zarządzania bezpieczeństwem informacji zgodnie z załącznikiem II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203;";

2) w art. 18 dodaje się lit. l) w brzmieniu:

„l) ustanawiają, wdrażają i utrzymują system zarządzania bezpieczeństwem informacji zgodnie z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203.".

Artykuł 16

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia 22 lutego 2026 r.

Natomiast w odniesieniu do instytucji zapewniającej służby żeglugi powietrznej w ramach EGNOS podlegającej rozporządzeniu wykonawczemu (UE) 2017/373 niniejsze rozporządzenie stosuje się od dnia 1 stycznia 2026 r.

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

Sporządzono w Brukseli dnia 27 października 2022 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca

ZAŁĄCZNIK I

BEZPIECZEŃSTWO INFORMACJI – WYMAGANIA DLA ORGANÓW

[CZĘŚĆ-IS.AR]

IS.AR.100 Zakres stosowania

W niniejszej części ustanawia się wymagania dotyczące zarządzania, które muszą spełnić właściwe organy, o których mowa w art. 2 ust. 2 niniejszego rozporządzenia.

Wymagania, które takie właściwe organy muszą spełnić w zakresie realizacji zadań związanych z certyfikacją, nadzorem i egzekwowaniem przepisów, określono w rozporządzeniach, o których mowa w art. 2 ust. 1 niniejszego rozporządzenia i w art. 2 rozporządzenia delegowanego (UE) 2022/1645.

IS.AR.200 System zarządzania bezpieczeństwem informacji (SZBI)

a) Aby osiągnąć cele określone w art. 1, właściwy organ ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji (SZBI) zapewniający, aby dany właściwy organ:

1) ustanowił strategię bezpieczeństwa informacji określającą ogólne zasady obowiązujące w danym właściwym organie w zakresie potencjalnego wpływu ryzyka związanego z bezpieczeństwem informacji na bezpieczeństwo lotnicze;

2) określił ryzyko związane z bezpieczeństwem informacji i dokonał przeglądu takiego ryzyka zgodnie z pkt IS.AR.205;

3) określił i wdrożył środki zmniejszające ryzyko związane z bezpieczeństwem informacji zgodnie z pkt IS.AR.210;

4) zdefiniował i wdrożył, zgodnie z pkt IS.AR.215, środki konieczne do wykrywania zdarzeń związanych z bezpieczeństwem informacji, identyfikował takie zdarzenia, które uznaje się za incydenty o potencjalnym wpływie na bezpieczeństwo lotnicze, oraz reagował na takie incydenty związane z bezpieczeństwem informacji i przywracał sytuację sprzed takich incydentów związanych z bezpieczeństwem informacji;

5) przestrzegał wymagań zawartych w pkt IS.AR.220 w przypadku zlecenia jakiejkolwiek części czynności opisanych w pkt IS.AR.200 innym organizacjom;

6) przestrzegał wymagań dotyczących personelu określonych w pkt IS.AR.225;

7) przestrzegał wymagań dotyczących prowadzenia rejestrów określonych w pkt IS.AR.230;

8) monitorował przestrzeganie przez własną organizację wymagań określonych w niniejszym rozporządzeniu oraz udzielał informacji zwrotnych dotyczących niezgodności osobie, o której mowa w pkt IS.AR.225 lit. a), w celu zapewnienia skutecznego wdrożenia działań naprawczych;

9) chronił poufność wszelkich informacji, które właściwy organ może posiadać w odniesieniu do organizacji objętej jego nadzorem, oraz informacji otrzymanych za pośrednictwem stosowanych przez organizację systemów zewnętrznego zgłaszania zdarzeń ustanowionych zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do niniejszego rozporządzenia oraz pkt IS.D.OR.230 załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645;

10) powiadomił Agencję o zmianach wpływających na zdolność właściwego organu do wykonywania powierzonych mu zadań i obowiązków określonych w niniejszym rozporządzeniu;

11) zdefiniował i wdrożył procedury wymiany istotnych informacji, w stosownych przypadkach i w sposób praktyczny i terminowy, w celu wspierania innych właściwych organów i agencji, a także organizacji objętych niniejszym rozporządzeniem, w procesie przeprowadzania skutecznej oceny ryzyka związanego z bezpieczeństwem w odniesieniu do wykonywanych przez nie czynności.

b) Aby zapewnić stałe przestrzeganie wymagań, o których mowa w art. 1, właściwy organ wdraża proces ciągłego doskonalenia zgodnie z pkt IS.AR.235.

c) Właściwy organ dokumentuje wszystkie najważniejsze procesy, procedury, funkcje i obowiązki konieczne do zapewnienia zgodności z pkt IS.AR.200 lit. a) oraz ustanawia tryb zmiany tej dokumentacji.

d) Procesy, procedury, funkcje i obowiązki utworzone przez właściwy organ w celu zapewnienia zgodności z pkt IS.AR.200 lit. a) odpowiadają charakterowi i złożoności działalności tego właściwego organu, na podstawie oceny właściwego dla tej działalności ryzyka związanego z bezpieczeństwem informacji, oraz mogą zostać włączone do innych systemów zarządzania już wdrożonych przez ten właściwy organ.

IS.AR.205 Ocena ryzyka związanego z bezpieczeństwem informacji

a) Właściwy organ identyfikuje wszystkie elementy własnej organizacji, które mogą być narażone na ryzyko związane z bezpieczeństwem informacji. Obejmuje to:

1) działalność, obiekty i zasoby właściwego organu, a także służby, które ten właściwy organ obsługuje, zapewnia, otrzymuje lub utrzymuje;

2) wyposażenie, układy, dane i informacje, które przyczyniają się do funkcjonowania elementów, o których mowa w pkt 1.

b) Właściwy organ powinien zidentyfikować interfejsy łączące jego własną organizację z innymi organizacjami, które to interfejsy mogą powodować wzajemne narażenie na ryzyko związane z bezpieczeństwem informacji.

c) Jeżeli chodzi o elementy i interfejsy, o których mowa w lit. a) i b), właściwy organ identyfikuje ryzyko związane z bezpieczeństwem informacji, które może mieć potencjalny wpływ na bezpieczeństwo lotnicze.

W odniesieniu do każdego zidentyfikowanego rodzaju ryzyka właściwy organ:

1) przypisuje poziom ryzyka zgodnie ze wstępnie określoną klasyfikacją ustanowioną przez dany właściwy organ;

2) przypisuje każdy rodzaj ryzyka i jego poziom odpowiedniemu elementowi lub interfejsowi określonemu zgodnie z lit. a) i b).

W ramach wstępnie określonej klasyfikacji, o której mowa w pkt 1, bierze się pod uwagę możliwość wystąpienia scenariusza zagrożenia i dotkliwość jego skutków dla bezpieczeństwa. Na podstawie tej klasyfikacji i biorąc pod uwagę kwestię, czy właściwy organ stosuje zorganizowany i powtarzalny proces zarządzania ryzykiem w odniesieniu do operacji, taki właściwy organ musi być w stanie ustalić, czy ryzyko jest dopuszczalne czy też wymaga zmniejszenia zgodnie z pkt IS.AR.210.

Aby umożliwić porównywalność różnych ocen ryzyka, przypisując poziom ryzyka na podstawie pkt 1, należy brać pod uwagę istotne informacje otrzymane w ramach współpracy z organizacjami, o których mowa w lit. b).

d) Właściwy organ przeprowadza przegląd oceny ryzyka przeprowadzonej zgodnie z lit. a), b) i c) i aktualizuje ją we wszystkich następujących sytuacjach:

1) w przypadku zmiany elementów narażonych na ryzyko związane z bezpieczeństwem informacji;

2) w przypadku zmiany interfejsów komunikacji między organizacją właściwego organu a innymi organizacjami lub ryzyka, o którym poinformowały pozostałe organizacje;

3) w przypadku zmiany informacji lub wiedzy wykorzystywanych do identyfikacji, analizy i klasyfikacji ryzyka;

4) gdy dostępne są wnioski z analizy incydentów związanych z bezpieczeństwem informacji.

IS.AR.210 Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

a) Właściwy organ opracowuje środki służące wyeliminowaniu niedopuszczalnego ryzyka zidentyfikowanego zgodnie z pkt IS.AR.205, terminowo wdraża te środki i kontroluje ich ciągłą skuteczność. Środki te umożliwiają właściwemu organowi:

1) kontrolowanie okoliczności, które przyczyniają się do faktycznego wystąpienia scenariusza zagrożenia;

2) ograniczenie skutków dla bezpieczeństwa lotniczego urzeczywistnienia się scenariusza zagrożenia;

3) uniknięcie ryzyka.

Środki te nie mogą stwarzać jakiegokolwiek nowego potencjalnego niedopuszczalnego ryzyka dla bezpieczeństwa lotniczego.

b) Osobę, o której mowa w pkt IS.AR.225 lit. a), oraz innych narażonych członków personelu właściwego organu należy powiadomić o wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.AR.205 oraz o powiązanych scenariuszach zagrożenia i wprowadzanych środkach.

Właściwy organ informuje również organizacje, z którymi jest połączony interfejsem zgodnie z pkt IS.AR.205 lit. b), o każdym rodzaju ryzyka wspólnym dla właściwego organu i organizacji.

IS.AR.215 Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze

a) Na podstawie wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.AR.205 i wyniku procesu zmniejszania ryzyka przeprowadzonego zgodnie z pkt IS.AR.210 właściwy organ wdraża środki służące do wykrywania zdarzeń, które wskazują na ewentualne urzeczywistnienie się niedopuszczalnego ryzyka i mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze. Dzięki takim środkom wykrywania właściwy organ może:

1) identyfikować odstępstwa od wcześniej określonych wartości bazowych dotyczących osiągów funkcjonalnych;

2) wysyłać ostrzeżenia służące uruchomieniu odpowiednich środków reagowania w przypadku każdego odstępstwa.

b) Właściwy organ wdraża środki reagowania na wszelkie zdarzenia zidentyfikowane zgodnie z lit. a), które mogą przerodzić się lub już przerodziły się w incydent związany z bezpieczeństwem informacji. Dzięki takim środkom reagowania właściwy organ może:

1) rozpocząć działanie własnej organizacji w reakcji na ostrzeżenia, o których mowa w lit. a) ppkt 2, poprzez uruchomienie wcześniej określonych zasobów i sposobu postępowania;

2) ograniczyć rozprzestrzenianie ataku i uniknąć pełnego urzeczywistnienia się scenariusza zagrożenia;

3) kontrolować tryb awaryjny uszkodzonych elementów określonych w pkt IS.AR.205 lit. a).

c) Właściwy organ wdraża środki służące przywróceniu stanu sprzed incydentów związanych z bezpieczeństwem informacji, w tym w razie potrzeby środki reagowania w sytuacjach zagrożeń. Dzięki takim środkom naprawczym właściwy organ może:

1) wyeliminować stan będący źródłem incydentu lub ograniczyć go do dopuszczalnego poziomu;

2) doprowadzić do bezpiecznego stanu uszkodzone elementy określone w pkt IS.AR.205 lit. a) w czasie naprawy wcześniej określonym przez jego własną organizację.

IS.AR.220 Zlecanie czynności w zakresie zarządzania bezpieczeństwem informacji

Właściwy organ zapewnia, aby w przypadku zlecenia innym organizacjom realizacji dowolnej części czynności, o których mowa w pkt IS.AR.200, zlecane czynności były zgodne z wymaganiami określonymi w niniejszym rozporządzeniu, a organizacja przyjmująca zlecenie wykonywała prace pod jego nadzorem. Właściwy organ zapewnia odpowiednie zarządzanie ryzykiem związanym ze zlecanymi czynnościami.

IS.AR.225 Wymagania dotyczące personelu

Właściwy organ:

a) wyznacza osobę uprawnioną do ustanowienia i utrzymania struktur organizacyjnych, strategii, procesów i procedur niezbędnych do wdrożenia niniejszego rozporządzenia.

Osoba ta:

1) jest uprawniona do uzyskania pełnego dostępu do zasobów niezbędnych właściwemu organowi do wykonywania wszystkich powierzonych mu zadań zgodnie z wymogami niniejszego rozporządzenia;

2) otrzymała uprawnienia niezbędne do wykonywania wyznaczonych obowiązków;

b) stosuje procedurę zapewniającą dysponowanie personelem dyżurującym wystarczającym do przeprowadzenia czynności objętych niniejszym załącznikiem;

c) stosuje procedurę zapewniającą, aby personel, o którym mowa w lit. b), posiadał niezbędne kompetencje do realizacji powierzonych mu zadań;

d) stosuje procedurę zapewniającą, aby personel przyjmował do wiadomości obowiązki związane z przydzielonymi funkcjami i zadaniami;

e) zapewnia, aby prawidłowo ustalono tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych podlegających wymaganiom niniejszego rozporządzenia.

IS.AR.230 Prowadzenie rejestrów

a) Właściwy organ prowadzi rejestr swoich działań w zakresie zarządzania bezpieczeństwem informacji.

1) Właściwy organ zapewnia, aby następujące zapisy były archiwizowane i możliwe do zidentyfikowania:

(i) umowy dotyczące czynności, o których mowa w pkt IS.AR.200 lit. a) ppkt 5;

(ii) rejestr najważniejszych procesów, o których mowa w pkt IS.AR.200 lit. d);

(iii) dokumentacja ryzyka zidentyfikowanego w ocenie ryzyka, o której mowa w pkt IS.AR.205, wraz z powiązanymi środkami zmniejszania ryzyka, o których mowa w pkt IS.AR.210;

(iv) dokumentacja zdarzeń związanych z bezpieczeństwem informacji, które mogą wymagać ponownej oceny w celu identyfikacji niewykrytych incydentów związanych z bezpieczeństwem informacji lub podatności.

2) Dokumentację, o której mowa w pkt 1 ppkt (i), przechowuje się przez co najmniej 5 lat od zmiany lub rozwiązania umowy.

3) Dokumentację, o której mowa w pkt 1 ppkt (ii) i (iii), przechowuje się przez co najmniej 5 lat.

4) Dokumentację, o której mowa w pkt 1 ppkt (iv), przechowuje się do czasu ponownej oceny zdarzeń związanych z bezpieczeństwem informacji, dokonywanej z częstotliwością określoną w ramach procedury ustanowionej przez właściwy organ.

b) Właściwy organ prowadzi rejestr kwalifikacji i doświadczenia własnego personelu zaangażowanego w czynności w zakresie zarządzania bezpieczeństwem informacji.

1) Dokumentację kwalifikacji i doświadczenia członków personelu przechowuje się przez cały okres zatrudnienia tych osób we właściwym organie i przez co najmniej 3 lata po opuszczeniu przez nie właściwego organu.

2) Członkowie personelu na żądanie otrzymują dostęp do swoich akt osobowych. Ponadto właściwy organ przekazuje członkom personelu na żądanie egzemplarz ich akt osobowych w chwili, gdy osoby te opuszczają właściwy organ.

c) Format dokumentacji musi być określony w procedurach właściwego organu.

d) Rejestry przechowuje się w sposób zapewniający ochronę przed uszkodzeniem, zmianą i kradzieżą, a informacje klasyfikowane, w razie potrzeby, w zależności od poziomu klauzuli tajności. Właściwy organ zapewnia przechowywanie rejestrów w sposób gwarantujący ich integralność, autentyczność i uprawniony dostęp.

IS.AR.235 Ciągłe doskonalenie

a) Właściwy organ dokonuje oceny – stosując odpowiednie wskaźniki skuteczności działania – skuteczności i stopnia zaawansowania własnego SZBI. Oceny tej dokonuje się według kalendarza wcześniej ustalonego przez właściwy organ lub po wystąpieniu incydentu związanego z bezpieczeństwem informacji.

b) Jeżeli w toku oceny przeprowadzonej zgodnie z lit. a) zostają wykryte uchybienia, właściwy organ wprowadza niezbędne środki poprawy w celu zapewnienia, aby system SZBI w dalszym ciągu był zgodny z mającymi zastosowanie wymaganiami i umożliwiał utrzymanie dopuszczalnego poziomu ryzyka związanego z bezpieczeństwem informacji. Ponadto właściwy organ ponownie ocenia elementy SZBI, na które przyjęte środki wpływają.

ZAŁĄCZNIK II

BEZPIECZEŃSTWO INFORMACJI — WYMAGANIA DLA ORGANIZACJI

[CZĘŚĆ IS.I.OR]

IS.I.OR.100 Zakres stosowania

W niniejszej części ustanawia się wymagania, które muszą spełnić organizacje, o których mowa w art. 2 ust. 1 niniejszego rozporządzenia.

IS.I.OR.200 System zarządzania bezpieczeństwem informacji (SZBI)

a) Aby osiągnąć cele określone w art. 1, organizacja ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji (SZBI) zapewniający, aby dana organizacja:

   1) ustanowiła strategię bezpieczeństwa informacji określającą ogólne zasady obowiązujące w danej organizacji w zakresie potencjalnego wpływu ryzyka związanego z bezpieczeństwem informacji na bezpieczeństwo lotnicze;

   2) określiła ryzyko związane z bezpieczeństwem informacji i dokonała przeglądu takiego ryzyka zgodnie z pkt IS.I.OR.205;

   3) określiła i wdrożyła środki zmniejszające ryzyko związane z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.210;

   4) wdrożyła system wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.215;

   5) zdefiniowała i wdrożyła, zgodnie z pkt IS.I.OR.220, środki konieczne do wykrywania zdarzeń związanych z bezpieczeństwem informacji, identyfikowała te zdarzenia, które uznaje się za incydenty o potencjalnym wpływie na bezpieczeństwo lotnicze, z wyjątkiem przypadków dopuszczonych w pkt IS.I.OR.205 lit. e), oraz reagowała na te incydenty związane z bezpieczeństwem informacji i przywracała sytuację sprzed takich incydentów związanych z bezpieczeństwem informacji;

6) wdrożyła środki, o których powiadomił właściwy organ, w ramach natychmiastowej reakcji na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze;

7) podjęła odpowiednie działanie, zgodnie z pkt IS.I.OR.225, aby wyeliminować niezgodności, o których powiadomił właściwy organ;

8) wdrożyła system zewnętrznego zgłaszania zdarzeń zgodnie z pkt IS.I.OR.230, aby właściwy organ mógł podjąć odpowiednie działania;

9) przestrzegała wymagań zawartych w pkt IS.I.OR.235 w przypadku zlecenia jakiejkolwiek części czynności, o których mowa w pkt IS.I.OR.200, innym organizacjom;

10) przestrzegała wymagań dotyczących personelu, określonych w pkt IS.I.OR.240;

11) przestrzegała wymagań dotyczących prowadzenia rejestrów określonych w pkt IS.I.OR.245;

12) monitorowała przestrzeganie przez organizację wymagań określonych w niniejszym rozporządzeniu oraz udzielała informacji zwrotnych dotyczących niezgodności kierownikowi odpowiedzialnemu w celu zapewnienia skutecznego wdrożenia działań naprawczych;

13) chroniła – bez uszczerbku dla mających zastosowanie wymagań dotyczących zgłaszania incydentów – poufność wszelkich informacji, które organizacja mogła otrzymać od innych organizacji, zgodnie z poziomem ich wrażliwości.

b) Aby zapewnić stałe przestrzeganie wymagań, o których mowa w art. 1, organizacja wdraża proces ciągłego doskonalenia zgodnie z pkt IS.I.OR.260.

c) Organizacja dokumentuje, zgodnie z pkt IS.I.OR.250, wszystkie najważniejsze procesy, procedury, funkcje i obowiązki konieczne do zapewnienia zgodności z pkt IS.I.OR.200 lit. a) oraz ustanawia tryb zmiany tej dokumentacji. Zarządzanie zmianami tych procesów, procedur, funkcji i obowiązków przebiega zgodnie z pkt IS.I.OR.255.

d) Procesy, procedury, funkcje i obowiązki utworzone przez organizację w celu zapewnienia zgodności z pkt IS.I.OR.200 lit. a) odpowiadają charakterowi i złożoności działalności tej organizacji, na podstawie oceny właściwego dla tej działalności ryzyka związanego z bezpieczeństwem informacji, oraz mogą zostać włączone do innych systemów zarządzania już wdrożonych przez tę organizację.

e) Bez uszczerbku dla obowiązku przestrzegania wymagań w zakresie zgłaszania zdarzeń zawartych w rozporządzeniu (UE) nr 376/2014 i wymagań określonych w pkt IS.I.OR.200 lit. a) ppkt 13 właściwy organ może zezwolić organizacji na niewdrożenie wymagań, o których mowa w lit. a)–d), oraz powiązanych wymagań określonych w pkt IS.I.OR.205 do IS.I.OR.260, jeżeli organizacja ta wykaże w sposób spełniający oczekiwania tego organu, że jej działalność, obiekty i zasoby, a także służby, które obsługuje, zapewnia, otrzymuje i utrzymuje, nie stwarzają żadnego ryzyka związanego z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze ani wobec tej organizacji, ani wobec innych organizacji. Takie zezwolenie musi opierać się na udokumentowanej ocenie ryzyka związanego z bezpieczeństwem informacji przeprowadzonej przez tę organizację lub przez stronę trzecią zgodnie z pkt IS.I.OR.205 oraz sprawdzonej i zatwierdzonej przez jej właściwy organ.

Właściwy organ będzie przeprowadzał przegląd ciągłości ważności takiego zatwierdzenia po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.

IS.I.OR.205 Ocena ryzyka związanego z bezpieczeństwem informacji

a) Organizacja identyfikuje wszystkie swoje elementy, które mogą być narażone na ryzyko związane z bezpieczeństwem informacji. Elementy te obejmują:

1) działalność, obiekty i zasoby organizacji, a także służby, które ta organizacja obsługuje, zapewnia, otrzymuje lub utrzymuje;

2) wyposażenie, układy, dane i informacje, które przyczyniają się do funkcjonowania elementów wymienionych w pkt 1.

b) Organizacja powinna zidentyfikować łączące ją z innymi organizacjami interfejsy, które mogą powodować wzajemne narażenie na ryzyko związane z bezpieczeństwem informacji.

c) Jeżeli chodzi o elementy i interfejsy, o których mowa w lit. a) i b), organizacja identyfikuje ryzyko związane z bezpieczeństwem informacji, które może mieć potencjalny wpływ na bezpieczeństwo lotnicze. W odniesieniu do każdego zidentyfikowanego rodzaju ryzyka organizacja:

1) przypisuje poziom ryzyka zgodnie ze wstępnie określoną klasyfikacją ustanowioną przez daną organizację;

2) przypisuje każdy rodzaj ryzyka i jego poziom odpowiedniemu elementowi lub interfejsowi określonemu zgodnie z lit. a) i b).

W ramach wstępnie określonej klasyfikacji, o której mowa w pkt 1, bierze się pod uwagę możliwość wystąpienia scenariusza zagrożenia i dotkliwość jego skutków dla bezpieczeństwa. Na podstawie tej klasyfikacji i biorąc pod uwagę kwestię, czy organizacja stosuje zorganizowany i powtarzalny proces zarządzania ryzykiem w odniesieniu do operacji, organizacja musi być w stanie ustalić, czy ryzyko jest dopuszczalne czy też wymaga zmniejszenia zgodnie z pkt IS.I.OR.210.

Aby umożliwić wzajemną porównywalność oceny ryzyka, przypisując poziom ryzyka na podstawie pkt 1, należy brać pod uwagę istotne informacje otrzymane we współpracy z organizacjami, o których mowa w lit. b).

d) Organizacja przeprowadza przegląd oceny ryzyka przeprowadzonej zgodnie z lit. a), b) i w stosownych przypadkach lit. c) lub e) oraz aktualizuje ją we wszystkich następujących sytuacjach:

1) w przypadku zmiany elementów narażonych na ryzyko związane z bezpieczeństwem informacji;

2) w przypadku zmiany interfejsów między organizacją a innymi organizacjami lub ryzyka, o którym poinformowały pozostałe organizacje;

3) w przypadku zmiany informacji lub wiedzy wykorzystywanych do identyfikacji, analizy i klasyfikacji ryzyka;

4) gdy dostępne są wnioski z analizy incydentów związanych z bezpieczeństwem informacji.

e) Na zasadzie odstępstwa od lit. c) organizacje zobowiązane do przestrzegania podczęści C załącznika III (część ATM/ANS.OR) do rozporządzenia wykonawczego (UE) 2017/373 zastępują analizę wpływu na bezpieczeństwo lotnicze analizą wpływu na ich służby zgodnie z dodatkową oceną bezpieczeństwa wymaganą w pkt ATM/ANS.OR.C.005. Ta dodatkowa ocena bezpieczeństwa zostaje udostępniona instytucjom zapewniającym służby ruchu lotniczego, które obsługują, a te instytucje zapewniające służby ruchu lotniczego odpowiadają za ocenę wpływu na bezpieczeństwo lotnicze.

IS.I.OR.210 Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

a) Organizacja opracowuje środki służące wyeliminowaniu niedopuszczalnego ryzyka zidentyfikowanego zgodnie z pkt IS.I.OR.205, terminowo wdraża te środki i kontroluje ich ciągłą skuteczność. Środki te umożliwiają organizacji:

1) kontrolowanie okoliczności, które przyczyniają się do faktycznego wystąpienia scenariusza zagrożenia;

2) ograniczenie skutków dla bezpieczeństwa lotniczego urzeczywistnienia się scenariusza zagrożenia;

3) uniknięcie ryzyka.

Środki te nie mogą stwarzać jakiegokolwiek nowego potencjalnego niedopuszczalnego ryzyka dla bezpieczeństwa lotniczego.

b) Osobę, o której mowa w pkt IS.I.OR.240 lit. a) i b), oraz innych narażonych członków personelu organizacji należy powiadomić o wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.I.OR.205 oraz o powiązanych scenariuszach zagrożenia i wprowadzanych środkach.

Organizacja informuje również organizacje, z którymi jest połączona interfejsem zgodnie z pkt IS.I.OR.205 lit. b), o każdym rodzaju ryzyka wspólnym dla obu organizacji.

IS.I.OR.215 System wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji

a) Organizacja ustanawia system wewnętrznego zgłaszania zdarzeń, aby móc gromadzić informacje o zdarzeniach związanych z bezpieczeństwem informacji, w tym o zdarzeniach zgłaszanych na podstawie pkt IS.I.OR.230, oraz oceniać takie zdarzenia.

b) Dzięki temu systemowi i procesowi, o którym mowa w pkt IS.I.OR.220, organizacja może:

1) określić, które zdarzenia zgłoszone na podstawie lit. a) uznaje się za incydenty związane z bezpieczeństwem informacji lub podatność o potencjalnym wpływie na bezpieczeństwo lotnicze;

2) określić przyczynę incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z pkt 1 oraz czynniki przyczyniające się do ich wystąpienia, a także uwzględnić je w procesie zarządzania ryzykiem związanym z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.205 i IS.I.OR.220;

3) zapewnić ocenę wszystkich znanych, istotnych informacji dotyczących incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z ppkt 1;

4) w razie potrzeby zapewnić wdrożenie metody wewnętrznej dystrybucji informacji.

c) Każda organizacja przyjmująca zlecenia, która może narazić organizację na ryzyko związane z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, jest zobowiązana do zgłaszania organizacji zdarzeń związanych z bezpieczeństwem informacji. Takie zgłoszenia są dokonywane z użyciem procedur ustanowionych w drodze szczegółowych uzgodnień umownych oraz podlegają ocenie zgodnie z lit. b).

d) Organizacja współpracuje w ramach badań z każdą inną organizacją, która w sposób istotny przyczynia się do bezpieczeństwa informacji dotyczącego działalności własnej.

e) Organizacja może zintegrować taki system zgłaszania zdarzeń z innymi systemami zgłaszania, które już wdrożyła.

IS.I.OR.220 Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze

a) Na podstawie wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.I.OR.205 i wyniku procesu zmniejszania ryzyka przeprowadzonego zgodnie z pkt IS.I.OR.210 organizacja wdraża środki służące wykrywaniu incydentów i podatności, które wskazują na ewentualne urzeczywistnienie się niedopuszczalnego ryzyka i mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze. Dzięki tym środkom wykrywania organizacja może:

1) identyfikować odstępstwa od wcześniej określonych wartości bazowych dotyczących osiągów funkcjonalnych;

2) wysyłać ostrzeżenia służące uruchomieniu odpowiednich środków reagowania w przypadku każdego odstępstwa.

b) Organizacja wdraża środki reagowania na wszelkie zdarzenia zidentyfikowane zgodnie z lit. a), które mogą przerodzić się lub już przerodziły się w incydent związany z bezpieczeństwem informacji. Dzięki tym środkom reagowania organizacja może:

1) rozpocząć działanie w reakcji na ostrzeżenia, o których mowa w lit. a) ppkt 2, poprzez uruchomienie wcześniej określonych zasobów i sposobu postępowania;

2) ograniczyć rozprzestrzenianie ataku i uniknąć pełnego urzeczywistnienia się scenariusza zagrożenia;

3) kontrolować tryb awaryjny uszkodzonych elementów określonych w pkt IS.I.OR.205 lit. a).

c) Organizacja wdraża środki służące przywróceniu stanu sprzed incydentów związanych z bezpieczeństwem informacji, w tym w razie potrzeby środki reagowania w sytuacjach zagrożeń. Dzięki tym środkom naprawczym organizacja może:

1) wyeliminować stan będący źródłem incydentu lub ograniczyć go do dopuszczalnego poziomu;

2) doprowadzić do bezpiecznego stanu uszkodzone elementy określone w pkt IS.I.OR.205 lit. a) w czasie naprawy wcześniej określonym przez organizację.

IS.I.OR.225 Reagowanie na niezgodności, o których powiadomił właściwy organ

a) Po otrzymaniu powiadomienia o niezgodnościach stwierdzonych przez właściwy organ organizacja:

1) identyfikuje przyczynę lub przyczyny niezgodności oraz czynniki sprzyjające jej wystąpieniu;

2) określa plan działań naprawczych;

3) wykazuje wyeliminowanie niezgodności w sposób spełniający oczekiwania właściwego organu.

b) Działania, o których mowa w lit. a), przeprowadza się w okresie uzgodnionym z właściwym organem.

IS.I.OR.230 System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji

a) Organizacja wdraża system zgłaszania zdarzeń związanych z bezpieczeństwem informacji, który jest zgodny z wymaganiami określonymi w rozporządzeniu (UE) nr 376/2014 i w jego aktach delegowanych i wykonawczych, jeżeli rozporządzenie to ma zastosowanie do danej organizacji.

b) Bez uszczerbku dla obowiązków określonych w rozporządzeniu (UE) nr 376/2014 organizacja zapewnia, aby każdy incydent związany z bezpieczeństwem informacji lub podatność, które mogą stanowić poważne ryzyko dla bezpieczeństwa lotniczego, zgłaszano właściwemu organowi, któremu podlega. Ponadto:

1) jeżeli taki incydent lub taka podatność ma wpływ na statek powietrzny lub powiązany system lub komponent, organizacja zgłasza taki incydent lub taką podatność również posiadaczowi zatwierdzenia projektu;

2) jeżeli taki incydent lub taka podatność ma wpływ na system lub część składową wykorzystywane przez organizację, organizacja ta zgłasza taki incydent lub taką podatność organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej.

c) Organizacja zgłasza stan, o którym mowa w lit. b), w następujący sposób:

1) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione powiadomienie, jak tylko organizacja dowie się o zaistnieniu danego stanu;

2) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione zgłoszenie w możliwie najszybszym trybie, ale nie później niż 72 godziny od chwili, w której organizacja dowiedziała się o zaistnieniu danego stanu, chyba że wyjątkowe okoliczności to uniemożliwią.

Zgłoszenia dokonuje się w formie określonej przez właściwy organ i zawiera ono wszystkie istotne informacje na temat znanego organizacji stanu;

3) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione zgłoszenie uzupełniające zawierające szczegóły działań, jakie organizacja podjęła lub zamierza podjąć w celu przywrócenia sytuacji sprzed incydentu, oraz działań, jakie zamierza podjąć w celu zapobieżenia występowaniu podobnych incydentów związanych z bezpieczeństwem informacji w przyszłości.

Zgłoszenie uzupełniające przedstawia się niezwłocznie po identyfikacji działań i w formie określonej przez właściwy organ.

IS.I.OR.235 Zlecanie czynności w zakresie zarządzania bezpieczeństwem informacji

a) Organizacja zapewnia, aby w przypadku zlecenia innym organizacjom realizacji dowolnej części czynności, o których mowa w pkt IS.I.OR.200, zlecane czynności były zgodne z wymaganiami określonymi w niniejszym rozporządzeniu, a organizacja przyjmująca zlecenie wykonywała prace pod jej nadzorem. Organizacja zapewnia odpowiednie zarządzanie ryzykiem związanym ze zlecanymi czynnościami.

b) Na żądanie organizacja zapewnia właściwemu organowi możliwość dostępu do organizacji przyjmującej zlecenie w celu ustalenia stałego przestrzegania mających zastosowanie wymagań określonych w niniejszym rozporządzeniu.

IS.I.OR.240 Wymagania dotyczące personelu

a) Kierownik odpowiedzialny w organizacji wyznaczony, odpowiednio, zgodnie z rozporządzeniami (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeniem wykonawczym (UE) 2017/373 lub rozporządzeniem wykonawczym (UE) 2021/664, o których to organizacjach jest mowa w art. 2 ust. 1 niniejszego rozporządzenia, posiada uprawnienia służbowe do zapewnienia możliwości finansowania i prowadzenia wszystkich czynności wymaganych w niniejszym rozporządzeniu. Osoba ta:

1) zapewnia dostępność wszystkich zasobów niezbędnych do zapewnienia zgodności z wymaganiami niniejszego rozporządzenia;

2) ustanawia i promuje strategię bezpieczeństwa informacji, o której mowa w pkt IS.I.OR.200 lit. a) ppkt 1;

3) jest w stanie wykazać się podstawową wiedzą na temat niniejszego rozporządzenia.

b) Kierownik odpowiedzialny wyznacza osobę lub grupę osób odpowiedzialnych za zapewnienie zgodności organizacji z wymaganiami niniejszego rozporządzenia oraz określa zakres kompetencji tych osób. Taka osoba lub grupa osób odpowiada bezpośrednio przed kierownikiem odpowiedzialnym oraz legitymuje się wiedzą, praktyką i doświadczeniem zawodowym odpowiednimi do powierzonego zakresu odpowiedzialności. W procedurach określa się, kto zastępuje daną osobę w przypadku jej długotrwałej nieobecności.

c) Kierownik odpowiedzialny wyznacza osobę lub grupę osób odpowiedzialnych za zarządzanie funkcją monitorowania zgodności, o której mowa w pkt IS.I.OR.200 lit. a) ppkt 12.

d) Jeżeli struktury organizacyjne, strategie, procesy i procedury w zakresie bezpieczeństwa informacji organizacji są wspólne z innymi organizacjami lub z obszarami własnej organizacji, które nie są objęte zatwierdzeniem ani deklaracją, kierownik odpowiedzialny może delegować swoje działania wspólnej osobie odpowiedzialnej.

W takim przypadku wprowadza się środki koordynacji między kierownikiem odpowiedzialnym organizacji a wspólną osobą odpowiedzialną w celu zapewnienia odpowiedniej integracji zarządzania bezpieczeństwem informacji w organizacji.

e) Kierownik odpowiedzialny lub wspólna osoba odpowiedzialna, o której mowa w lit. d), posiada uprawnienia służbowe do ustanowienia i utrzymania struktur organizacyjnych, strategii, procesów i procedur niezbędnych do wdrożenia pkt IS.I.OR.200.

f) Organizacja stosuje procedurę zapewniającą dysponowanie personelem dyżurującym wystarczającym do przeprowadzenia czynności objętych niniejszym załącznikiem.

g) Organizacja stosuje procedurę zapewniającą posiadanie przez personel, o którym mowa w lit. f), kompetencji niezbędnych do realizacji powierzonych mu zadań.

h) Organizacja stosuje procedurę zapewniającą przyjmowanie przez personel do wiadomości obowiązków związanych z przydzielonymi funkcjami i zadaniami.

i) Organizacja zapewnia, aby prawidłowo ustalono tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych podlegających wymaganiom niniejszego rozporządzenia.

IS.I.OR.245 Prowadzenie rejestrów

a) *Organizacja prowadzi rejestr swoich działań w zakresie zarządzania bezpieczeństwem informacji.*

1) Organizacja zapewnia, aby następujące zapisy były archiwizowane i możliwe do zidentyfikowania:

(i) każde otrzymane zatwierdzenie i każda powiązana ocena ryzyka związanego z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.200 lit. e);

(ii) umowy dotyczące czynności, o których mowa w pkt IS.I.OR.200 lit. a) ppkt 9;

(iii) rejestr najważniejszych procesów, o których mowa w pkt IS.I.OR.200 lit. d);

(iv) dokumentacja ryzyka zidentyfikowanego w ocenie ryzyka, o której mowa w pkt IS.I.OR.205, wraz z powiązanymi środkami zmniejszania ryzyka, o których mowa w pkt IS.I.OR.210;

(v) dokumentacja incydentów związanych z bezpieczeństwem informacji i podatności zgłoszonych za pośrednictwem systemów zgłaszania zdarzeń, o których mowa w pkt IS.I.OR.215 i IS.I.OR.230;

(vi) dokumentacja zdarzeń związanych z bezpieczeństwem informacji, które mogą wymagać ponownej oceny w celu identyfikacji niewykrytych incydentów związanych z bezpieczeństwem informacji lub podatności.

2) Dokumentację, o której mowa w pkt 1 ppkt (i), przechowuje się przez co najmniej 5 lat od utraty ważności zatwierdzenia.

3) Dokumentację, o której mowa w pkt 1 ppkt (ii), przechowuje się przez co najmniej 5 lat od zmiany lub rozwiązania umowy.

4) Dokumentację, o której mowa w pkt 1 ppkt (iii), (iv) i (v), przechowuje się przez co najmniej 5 lat.

5) Dokumentację, o której mowa w pkt 1 ppkt (vi), przechowuje się do czasu ponownej oceny zdarzeń związanych z bezpieczeństwem informacji, dokonywanej z częstotliwością określoną w ramach procedury ustanowionej przez organizację.

b) *Organizacja prowadzi rejestr kwalifikacji i doświadczenia własnego personelu zaangażowanego w działania w zakresie zarządzania bezpieczeństwem informacji.*

1) Dokumentację kwalifikacji i doświadczenia członków personelu przechowuje się przez cały okres zatrudnienia tych osób w organizacji i przez co najmniej 3 lata po opuszczeniu przez nie organizacji.

2) Członkowie personelu na żądanie otrzymują dostęp do swoich akt osobowych. Ponadto organizacja przekazuje członkom personelu na żądanie egzemplarz ich akt osobowych w chwili, gdy osoby te opuszczają organizację.

c) Format dokumentacji musi być określony w procedurach organizacji.

d) Rejestry przechowuje się w sposób zapewniający ochronę przed uszkodzeniem, zmianą i kradzieżą, a informacje klasyfikowane, w razie potrzeby, w zależności od poziomu klauzuli tajności. Właściwy organ zapewnia przechowywanie rejestrów w sposób gwarantujący ich integralność, autentyczność i uprawniony dostęp.

IS.I.OR.250 Podręcznik zarządzania bezpieczeństwem informacji

a) Organizacja udostępnia właściwemu organowi podręcznik zarządzania bezpieczeństwem informacji oraz, w stosownych przypadkach, wszelkie przywołane powiązane podręczniki i procedury, zawierający:

1) oświadczenie podpisane przez kierownika odpowiedzialnego, potwierdzające, że organizacja będzie zawsze będzie prowadzić prace zgodnie z niniejszym załącznikiem i podręcznikiem zarządzania bezpieczeństwem informacji. Jeżeli kierownik odpowiedzialny nie jest dyrektorem generalnym organizacji, wówczas taki dyrektor generalny musi kontrasygnować to oświadczenie;

2) tytuł(-y), imię(imiona) i nazwisko(-a), obowiązki, zakresy odpowiedzialności, zadania i uprawnienia osoby lub osób zdefiniowanych w pkt IS.I.OR.240 lit. b) i c);

3) w stosownych przypadkach tytuł, imię i nazwisko, obowiązki, zakresy odpowiedzialności, zadania i uprawnienia wspólnej osoby odpowiedzialnej zdefiniowanej w pkt IS.I.OR.240 lit. d);

4) stosowaną przez organizację strategię bezpieczeństwa informacji, o której mowa w pkt IS.I.OR.200 lit. a) ppkt 1;

5) ogólny opis liczby i kategorii pracowników oraz wprowadzonego systemu umożliwiającego planowanie dostępności pracowników zgodnie z wymaganiami pkt IS.I.OR.240;

6) tytuł(-y), imię(imiona) i nazwisko(-a), obowiązki, zakresy odpowiedzialności, zadania i uprawnienia kluczowych osób odpowiedzialnych za realizację pkt IS.I.OR.200, w tym osoby lub osób odpowiedzialnych za funkcję monitorowania zgodności, o której mowa w pkt IS.I.OR.200 lit. a) ppkt 12;

7) schemat organizacyjny ukazujący powiązaną strukturę odpowiedzialności w odniesieniu do osób, o których mowa w ppkt 2 i 6;

8) opis systemu wewnętrznego zgłaszania zdarzeń, o którym mowa w pkt IS.I.OR.215;

9) procedury wskazujące, w jaki sposób organizacja zapewnia zgodność z niniejszą częścią, a w szczególności:

(i) dokumentację, o której mowa w pkt IS.I.OR.200 lit. c);

(ii) procedury określające, w jaki sposób organizacja kontroluje wszelkie zlecane czynności, o których mowa w pkt IS.I.OR.200 lit. a) ppkt 9;

(iii) procedurę zmiany podręcznika zarządzania bezpieczeństwem informacji, o której mowa w lit. c);

10) szczegóły aktualnie zatwierdzonych alternatywnych sposobów spełnienia wymagań.

b) Właściwy organ zatwierdza pierwsze wydanie podręcznika zarządzania bezpieczeństwem informacji i zachowuje jego egzemplarz. W razie potrzeby w podręczniku zarządzania bezpieczeństwem informacji wprowadza się zmiany niezbędne do zachowania aktualnego opisu SZBI organizacji. Właściwy organ otrzymuje egzemplarz wszelkich zmian w podręczniku zarządzania bezpieczeństwem informacji.

c) Zarządzanie zmianami podręcznika zarządzania bezpieczeństwem informacji przebiega zgodnie z procedurą ustanowioną przez organizację. Wszelkie zmiany nieobjęte zakresem stosowania tej procedury, jak również wszelkie zmiany związane ze zmianami, o których mowa w pkt IS.I.OR.255 lit. b), podlegają zatwierdzeniu przez właściwy organ.

d) Organizacja może włączyć podręcznik zarządzania bezpieczeństwem informacji do innych posiadanych charakterystyk i podręczników zarządzania, pod warunkiem że stosuje się wyraźne odniesienia wskazujące, które części charakterystyki lub podręcznika zarządzania odnoszą się do poszczególnych wymagań zawartych w niniejszym załączniku.

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

a) Zarządzanie zmianami w SZBI i powiadamianie o nich właściwego organu może przebiegać w ramach procedury opracowanej przez organizację. Procedurę tę zatwierdza właściwy organ.

b) Jeżeli chodzi o zmiany w SZBI nieobjęte procedurą, o której mowa w lit. a), organizacja ubiega się o zatwierdzenie wydawane przez właściwy organ i musi je uzyskać.

W odniesieniu do tych zmian:

1) wniosek składa się przed wprowadzeniem wszelkich zmian w celu umożliwienia właściwemu organowi stwierdzenia, czy zachowana zostanie zgodność z niniejszym rozporządzeniem, oraz – jeśli zajdzie taka potrzeba – zmiany certyfikatu organizacji szkoleniowej i powiązanych warunków zatwierdzania dołączonych do certyfikatu;

2) organizacja przekazuje właściwemu organowi wszelkie informacje, których organ ten zażąda w celu dokonania oceny zmiany;

3) zmianę wprowadza się wyłącznie po otrzymaniu formalnego zatwierdzenia przez właściwy organ;

4) organizacja wprowadza tego typu zmiany zgodnie z warunkami określonymi przez właściwy organ.

IS.I.OR.260 Ciągłe doskonalenie

a) Stosując odpowiednie wskaźniki skuteczności działania, organizacja dokonuje oceny skuteczności i stopnia zaawansowania SZBI. Oceny tej dokonuje się według kalendarza wcześniej ustalonego przez organizację lub po wystąpieniu incydentu związanego z bezpieczeństwem informacji.

b) Jeżeli w toku oceny przeprowadzonej zgodnie z lit. a) zostają wykryte uchybienia, organizacja podejmuje niezbędne środki poprawy w celu utrzymania zgodności systemu SZBI z mającymi zastosowanie wymaganiami i umożliwienia utrzymania dopuszczalnego poziomu ryzyka związanego z bezpieczeństwem informacji. Ponadto organizacja ponownie ocenia elementy SZBI, na które przyjęte środki wpływają.

ZAŁĄCZNIK III

W załącznikach VI (część ARA) i VII (część ORA) do rozporządzenia (UE) nr 1178/2011 wprowadza się następujące zmiany:

1) w załączniku VI (część ARA) wprowadza się następujące zmiany:

a) w pkt ARA.GEN.125 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

b) po pkt ARA.GEN.135 dodaje się pkt ARA.GEN.135A w brzmieniu:

„**ARA.GEN.135A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt ARA.GEN.125 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

c) w pkt ARA.GEN.200 dodaje się lit. e) w brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

d) w pkt ARA.GEN.205 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„**ARA.GEN.205 Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ORA.GEN.200A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji ustanowiony zgodnie z pkt ARA.GEN.200 lit. e) obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

e) w pkt ARA.GEN.300 dodaje się lit. g) w brzmieniu:

„g) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ORA.GEN.200A, oprócz przestrzegania przepisów ustanowionych w lit. a)–f), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

f) po pkt ARA.GEN.330 dodaje się pkt ARA.GEN.330A w brzmieniu:

„**ARA.GEN.330A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W odniesieniu do zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określoną w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt ARA.GEN.300. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt ARA.GEN.350.

b) W odniesieniu do innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.";

2) w załączniku VII (część ORA) wprowadza się następujące zmiany:

po pkt ORA.GEN.200 dodaje się pkt ORA.GEN.200A w brzmieniu:

„**ORA.GEN.200A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt ORA.GEN.200, organizacja ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.".

ZAŁĄCZNIK IV

W załączniku I (część 21) do rozporządzenia (UE) nr 748/2012 wprowadza się następujące zmiany:

1) w spisie treści wprowadza się następujące zmiany:

   a) po nagłówku 21.B.20 dodaje się nagłówek w brzmieniu:

      „21.B.20A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze";

   b) nagłówek pkt 21.B.30 otrzymuje brzmienie:

      „21.B.30 Przydzielanie zadań";

   c) po nagłówku 21.B.240 dodaje się nagłówek w brzmieniu:

      „21.B.240A Zmiany w systemie zarządzania bezpieczeństwem informacji";

   d) po nagłówku 21.B.435 dodaje się nagłówek w brzmieniu:

      „21.B.435A Zmiany w systemie zarządzania bezpieczeństwem informacji";

2) w pkt 21.B.15 dodaje się lit. c) w brzmieniu:

   „c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.D.OR.230 załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645.";

3) po pkt 21.B.20 dodaje się pkt 21.B.20A w brzmieniu:

   „**21.B.20A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

   a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

   b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt 21.B.15 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

   c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

   d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

4) w pkt 21.B.25 dodaje się lit. e) w brzmieniu:

   „e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

5) w pkt 21.B.30 wprowadza się następujące zmiany:

a) nagłówek otrzymuje brzmienie:

„**21.B.30 Przydzielanie zadań”;**

b) dodaje się lit. c) w brzmieniu:

„c) Do celów certyfikacji i nadzoru nad zgodnością organizacji z pkt 21.A.139A i 21.A.239A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji ustanowiony zgodnie z pkt 21.B.25 lit. e) obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.”;

6) w pkt 21.B.221 dodaje się lit. g) w brzmieniu:

„g) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt 21.A.139A, oprócz przestrzegania przepisów ustanowionych w lit. a)–f), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.”;

7) po pkt 21.B.240 dodaje się pkt 21.B.240A w brzmieniu:

„**21.B.240A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określoną w pkt IS.D.OR.255 lit. a) załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt 21.B.221. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt 21.B.225.

b) W przypadku innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.D.OR.255 lit. b) załącznika I (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.”;

8) w pkt 21.B.431 dodaje się lit. d) w brzmieniu:

„d) Do celów certyfikacji i nadzoru nad zgodnością organizacji z pkt 21.A.239A, oprócz przestrzegania przepisów zawartych w lit. a)–c), właściwy organ stosuje się do następujących zasad:

1) właściwy organ dokonuje przeglądu interfejsów i powiązanego ryzyka zidentyfikowanych zgodnie z pkt IS.D.OR.205 lit. b) załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645 przez każdą organizację podlegającą jego nadzorowi;

2) w przypadku stwierdzenia przez poszczególne organizacje rozbieżności dotyczących wzajemnych interfejsów i powiązanego ryzyka właściwy organ dokonuje wraz z zainteresowanymi organizacjami przeglądu tych rozbieżności i, w stosownych przypadkach, zgłasza odpowiednie ustalenia, aby zapewnić wdrożenie działań naprawczych;

3) w przypadku gdy dokumentacja poddana przeglądowi zgodnie z pkt 2 ujawnia występowanie znaczącego ryzyka powiązanego z interfejsami między organizacjami podlegającymi nadzorowi innego właściwego organu w tym samym państwie członkowskim, informacja ta jest przekazywana odpowiedniemu właściwemu organowi.";

9) po pkt 21.B.435 dodaje się pkt 21.B.435A w brzmieniu:

„**21.B.435A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określoną w pkt IS.D.OR.255 lit. a) załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt 21.B.431. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt 21.B.433.

b) W przypadku innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.D.OR.255 lit. b) załącznika I (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.".

ZAŁĄCZNIK V

W załącznikach II (część ARO) i III (część ORAO) do rozporządzenia (UE) nr 965/2012 wprowadza się następujące zmiany:

1) w załączniku II (część ARO) wprowadza się następujące zmiany:

a) w pkt ARO.GEN.125 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

b) po pkt ARO.GEN.135 dodaje się pkt ARO.GEN.135A w brzmieniu:

„**ARO.GEN.135A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt ARO.GEN.125 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

c) w pkt ARO.GEN.200 dodaje się lit. e) w brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

d) w załączniku ARO.GEN.205 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„**ARO.GEN.205 Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) Do celów certyfikacji i nadzoru nad zgodnością organizacji z pkt ORO.GEN.200A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji, ustanowiony zgodnie z pkt ARO.GEN.200 lit. e), obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

e) w pkt ARO.GEN.300 dodaje się lit. g) w brzmieniu:

„g) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ORO.GEN.200A, oprócz przestrzegania przepisów ustanowionych w lit. a)–f), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

f) po pkt ARO.GEN.330 dodaje się pkt ARO.GEN.330A w brzmieniu:

„**ARO.GEN.330A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określona w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt ARO.GEN.300. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt ARO.GEN.350.

b) W przypadku innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.";

2) w załączniku III (część ORO) wprowadza się następujące zmiany:

po pkt ORO.GEN.200 dodaje się pkt ORO.GEN.200A w brzmieniu:

„**ORO.GEN.200A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt ORO.GEN.200, operator ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.".

ZAŁĄCZNIK VI

W załączniku II (część ADR.AR) do rozporządzenia (UE) nr 139/2014 wprowadza się następujące zmiany:

1) w pkt ADR.AR.A.025 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.D.OR.230 załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645.";

2) po pkt ADR.AR.A.030 dodaje się pkt ADR.AR.A.030A w brzmieniu:

„**ADR.AR.A.030A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt ADR.AR.A.025 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

3) w pkt ADR.AR.B.005 dodaje się lit. d) w brzmieniu:

„d) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

4) w pkt ADR.AR.B.010 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„**ADR.AR.B.010 Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ADR.OR.D.005A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji, ustanowiony zgodnie z pkt ADR.AR.B.005 lit. e), obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

5) w pkt ADR.AR.C.005 dodaje się lit. f) w brzmieniu:

„f) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ADR.OR.D.005A, oprócz przestrzegania przepisów ustanowionych w lit. a)–e), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

6) po pkt ADR.AR.C.040 dodaje się pkt ADR.AR.C.040A w brzmieniu:

„**ADR.AR.C.040A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W odniesieniu do zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określoną w pkt IS.D.OR.255 lit. a) załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt ADR.AR.C.005. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt ADR.AR.C.055.

b) W odniesieniu do innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.D.OR.255 lit. b) załącznika (część IS.D.OR) do rozporządzenia delegowanego (UE) 2022/1645:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.".

ZAŁĄCZNIK VII

W załącznikach II (część 145), III (część 66) i Vc (część CAMO) do rozporządzenia (UE) nr 1321/2014 wprowadza się następujące zmiany:

1) W załączniku II (część 145) wprowadza się następujące zmiany:

a) w spisie treści wprowadza się następujące zmiany:

(i) po nagłówku 145.A.200 dodaje się nagłówek w brzmieniu:

„145.A.200A System zarządzania bezpieczeństwem informacji";

(ii) po nagłówku 145.B.135 dodaje się nagłówek w brzmieniu:

„145.B.135A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze";

(iii) nagłówek pkt 145.B.205 otrzymuje brzmienie:

„145.B.205 Przydzielanie zadań";

(iv) po nagłówku 145.B.330 dodaje się nagłówek w brzmieniu:

„145.B.330A Zmiany w systemie zarządzania bezpieczeństwem informacji";

b) po pkt 145.A.200 dodaje się pkt 145.A.200A w brzmieniu:

„145.A.200A **System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt 145.A.200, organizacja obsługi technicznej ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

c) w pkt 145.B.125 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

d) po pkt 145.B.135 dodaje się pkt 145.B.135A w brzmieniu:

„145.B.135A **Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt 145.B.125 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

e) w pkt 145.B.200 dodaje się lit. e) w brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

f) w pkt 145.B.205 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„145.B.205 **Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) Do celów certyfikacji i nadzoru nad zgodnością organizacji z pkt 145.A.200A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji, ustanowiony zgodnie z pkt 145.B.200 lit. e), obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

g) w pkt 145.B.300 dodaje się lit. g) w brzmieniu:

„g) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ATM/145.A.200A, oprócz przestrzegania przepisów ustanowionych w lit. a)–c), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

h) po pkt 145.B.330 dodaje się pkt 145.B.330A w brzmieniu:

„145.B.330A **Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określona w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt 145.B.300. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt 145.B.350.

b) W przypadku innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.";

2) w załączniku III (część 66) wprowadza się następujące zmiany:

a) w spisie treści po nagłówku 66.B.10 dodaje się nagłówek w brzmieniu:

„66.B.15 System zarządzania bezpieczeństwem informacji";

b) po pkt 66.B.10 dodaje się pkt 66.B.15 w brzmieniu:

„66.B.15 **System zarządzania bezpieczeństwem informacji**

Właściwy organ ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

3) w załączniku Vc (część CAMO) wprowadza się następujące zmiany:

a) w spisie treści wprowadza się następujące zmiany:

(i) po nagłówku CAMO.A.200 dodaje się nagłówek w brzmieniu:

„CAMO.A.200A System zarządzania bezpieczeństwem informacji";

(ii) po nagłówku CAMO.B.135 dodaje się nagłówek w brzmieniu:

„CAMO.B.135A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze";

(iii) nagłówek pkt CAMO.B.205 otrzymuje brzmienie:

„CAMO.B.205 Przydzielanie zadań";

(iv) po nagłówku CAMO.B.330 dodaje się nagłówek w brzmieniu:

„CAMO.B.330A Zmiany w systemie zarządzania bezpieczeństwem informacji";

b) po pkt CAMO.A.200 dodaje się pkt CAMO.A.200A w brzmieniu:

„CAMO.A.200A **System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt CAMO.A.200, organizacja ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

c) w pkt CAMO.B.125 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

d) po pkt CAMO.B.135 dodaje się pkt CAMO.B.135A w brzmieniu:

„CAMO.B.135A **Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt CAMO.B.125 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub niezbędne działania naprawcze, które należy podjąć, by mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

e) w pkt CAMO.B.200 dodaje się lit. e) w brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

f) w pkt CAMO.B.205 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„CAMO.B.205 **Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt CAMO.A.200A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji ustanowiony zgodnie z pkt CAMO.B.200 lit. e) obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

g) w pkt CAMO.B.300 dodaje się lit. g) w brzmieniu:

„g) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt CAMO.A.200A, oprócz przestrzegania przepisów ustanowionych w lit. a)–f), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

h) po pkt CAMO.B.330 dodaje się pkt CAMO.B.330A w brzmieniu:

„CAMO.B.330A **Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określona w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt CAMO.B.300. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt CAMO.B.350.

b) W przypadku innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.".

ZAŁĄCZNIK VIII

W załącznikach II (część ATCO.AR) i III (część ATCO.OR) do rozporządzenia (UE) 2015/340 wprowadza się następujące zmiany:

1) w załączniku II (część ATCO.AR) wprowadza się następujące zmiany:

a) w pkt ATCO.AR.A.020 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

b) po pkt ATCO.AR.A.025 dodaje się pkt ATCO.AR.A.025A w brzmieniu:

„**ATCO.AR.A.025A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt ATCO.AR.A.020, oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub działania naprawcze, które należy podjąć, niezbędne do tego, aby mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

c) w pkt ATCO.AR.B.001 dodaje się lit. e) w brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

d) w pkt ATCO.AR.B.005 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„**ATCO.AR.B.005 Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ATCO.OR.C.001A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji ustanowiony zgodnie z pkt ATCO.AR.B.001 lit. e) obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

e) w pkt ATCO.AR.C.001 dodaje się lit. f) w brzmieniu:

„f) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ATCO.OR.C.001A, oprócz przestrzegania przepisów ustanowionych w lit. a)–e), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

f) po pkt ATCO.AR.E.010 dodaje się pkt ATCO.AR.E.010A w brzmieniu:

„**ATCO.AR.E.010A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W odniesieniu do zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określoną w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt ATCO.AR.C.001. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt ATCO.AR.C.010.

b) W odniesieniu do innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.";

2) w załączniku III (część ATCO.OR) wprowadza się następujące zmiany:

po pkt ATCO.OR.C.001 dodaje się pkt ATCO.OR.C.001A w brzmieniu:

„**ATCO.OR.C.001A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt ATCO.OR.C.001, organizacja szkoleniowa ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.".

ZAŁĄCZNIK IX

W załącznikach II (część ATM/ANS.AR) i III (część ATM/ANS.OR) do rozporządzenia wykonawczego (UE) 2017/373 wprowadza się następujące zmiany:

1) w załączniku II (część ATM/ANS.AR) wprowadza się następujące zmiany:

a) w pkt ATM/ANS.AR.A.020 dodaje się lit. c) w brzmieniu:

„c) Właściwy organ państwa członkowskiego jak najszybciej przekazuje Agencji informacje istotne z punktu widzenia bezpieczeństwa wynikające ze zgłoszeń zdarzeń związanych z bezpieczeństwem informacji, które otrzymał zgodnie z pkt IS.I.OR.230 załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203.";

b) po pkt ATM/ANS.AR.A.025 dodaje się pkt ATM/ANS.AR.A.025A w brzmieniu:

„**ATM/ANS.AR.A.025A Natychmiastowa reakcja na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze**

a) Właściwy organ wdraża system mający na celu odpowiednie gromadzenie, analizowanie i rozpowszechnianie informacji dotyczących zgłaszanych przez organizacje incydentów związanych z bezpieczeństwem informacji oraz podatności, które mogą mieć wpływ na bezpieczeństwo lotnicze. Odbywa się to w porozumieniu z wszelkimi innymi odpowiednimi organami odpowiedzialnymi za bezpieczeństwo informacji lub cyberbezpieczeństwo w danym państwie członkowskim w celu zwiększenia koordynacji i zgodności systemów zgłaszania zdarzeń.

b) Agencja wdraża system mający na celu odpowiednią analizę wszelkich odpowiednich informacji istotnych z punktu widzenia bezpieczeństwa, otrzymanych zgodnie z pkt ATM/ANS.AR.A.020 lit. c), oraz bez zbędnej zwłoki przekazuje państwom członkowskim i Komisji wszelkie informacje, w tym zalecenia lub działania naprawcze, które należy podjąć, niezbędne do tego, aby mogły one w odpowiednim czasie zareagować na incydent związany z bezpieczeństwem informacji lub podatność mające potencjalny wpływ na bezpieczeństwo lotnicze, dotyczące wyrobów, części, wyposażenia nieinstalowanego, osób lub organizacji podlegających rozporządzeniu (UE) 2018/1139 oraz aktom delegowanym i wykonawczym do tego rozporządzenia.

c) Po otrzymaniu informacji, o których mowa w lit. a) i b), właściwy organ wprowadza odpowiednie środki, aby wyeliminować potencjalny wpływ incydentu związanego z bezpieczeństwem informacji lub podatności na bezpieczeństwo lotnicze.

d) O środkach wprowadzanych zgodnie z lit. c) niezwłocznie informowane są wszystkie osoby lub organizacje, które są zobowiązane do ich przestrzegania na mocy rozporządzenia (UE) 2018/1139 oraz aktów delegowanych i wykonawczych do tego rozporządzenia. Właściwy organ państwa członkowskiego powiadamia również o tych środkach Agencję oraz, w razie konieczności podjęcia wspólnych działań, właściwe organy pozostałych zainteresowanych państw członkowskich.";

c) w pkt ATM/ANS.AR.B.001 dodaje się lit. e) w następującym brzmieniu:

„e) Oprócz spełniania wymagań określonych w lit. a) system zarządzania ustanowiony i utrzymywany przez właściwy organ musi być zgodny z załącznikiem I (część IS.AR) do rozporządzenia wykonawczego (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

d) w pkt ATM/ANS.AR.B.005 wprowadza się następujące zmiany:

(i) nagłówek otrzymuje brzmienie:

„**ATM/ANS.AR.B.005 Przydzielanie zadań**";

(ii) dodaje się lit. c) w brzmieniu:

„c) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ATM/ANS.OR.B.005A właściwy organ może przydzielić zadania kwalifikowanym jednostkom zgodnie z lit. a) lub każdemu odpowiedniemu organowi w danym państwie członkowskim odpowiedzialnemu za bezpieczeństwo informacji lub cyberbezpieczeństwo. Przydzielając zadania, właściwy organ musi dopilnować, aby:

1) kwalifikowana jednostka lub odpowiedni organ koordynowały i uwzględniały wszystkie aspekty związane z bezpieczeństwem lotniczym;

2) do ogólnej dokumentacji organizacji dotyczącej certyfikacji i nadzoru włączono wyniki działań w zakresie certyfikacji i nadzoru prowadzonych przez kwalifikowaną jednostkę lub odpowiedni organ;

3) jego własny system zarządzania bezpieczeństwem informacji ustanowiony zgodnie z pkt ATM/ANS.AR.B.001 lit. e) obejmował wszystkie zadania związane z certyfikacją i stałym nadzorem wykonywane w jego imieniu.";

e) w pkt ATM/ANS.AR.C.010 dodaje się lit. d) w brzmieniu:

„d) W odniesieniu do certyfikacji i nadzoru nad zgodnością organizacji z pkt ATM/ANS.OR.B.005A, oprócz przestrzegania przepisów ustanowionych w lit. a)–c), właściwy organ przeprowadza przegląd wszelkich zatwierdzeń wydanych zgodnie z pkt IS.I.OR.200 lit. e) niniejszego rozporządzenia lub pkt IS.D.OR.200 lit. e) rozporządzenia delegowanego (UE) 2022/1645 po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.";

f) po pkt ATM/ANS.AR.C.025 dodaje się pkt ATM/ANS.AR.C.025A w brzmieniu:

„**ATM/ANS.AR.C.025A Zmiany w systemie zarządzania bezpieczeństwem informacji**

a) W przypadku zmian zarządzanych i zgłaszanych właściwemu organowi zgodnie z procedurą określona w pkt IS.I.OR.255 lit. a) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203 właściwy organ uwzględnia przegląd takich zmian w stałym nadzorze sprawowanym zgodnie z zasadami określonymi w pkt ATM/ANS.AR.C.010. W przypadku stwierdzenia jakiejkolwiek niezgodności właściwy organ powiadamia o tym organizację, żąda dalszych zmian i podejmuje działania zgodnie z pkt ATM/ANS.AR.C.050.

b) W odniesieniu do innych zmian wymagających złożenia wniosku o zatwierdzenie zgodnie z pkt IS.I.OR.255 lit. b) załącznika II (część IS.I.OR) do rozporządzenia wykonawczego (UE) 2023/203:

1) po otrzymaniu wniosku o wprowadzenie zmiany przed wydaniem zatwierdzenia właściwy organ sprawdza czy organizacja spełnia stosowne wymagania;

2) właściwy organ ustala warunki, na jakich organizacja może działać w trakcie wprowadzania zmiany;

3) w przypadku stwierdzenia, że organizacja spełnia stosowne wymagania, właściwy organ zatwierdza zmianę.";

2) w załączniku III (część ATM/ANS.OR) wprowadza się następujące zmiany:

a) po pkt ATM/ANS.OR.B.005 dodaje się pkt ATM/ANS.OR.B.005A w brzmieniu:

„**ATM/ANS.OR.B.005A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania, o którym mowa w pkt ATM/ANS.OR.B.005, instytucja zapewniająca służby ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem wykonawczym (UE) 2023/203 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

b) pkt ATM/ANS.OR.D.010 otrzymuje brzmienie:

„**ATM/ANS.OR.D.010 Zarządzanie ochroną**

a) Instytucje zapewniające służby żeglugi powietrznej, instytucje zapewniające zarządzanie przepływem ruchu lotniczego oraz menedżer sieci ustanawiają, jako integralną część ich systemu zarządzania zgodnie z wymaganiami określonymi w pkt ATM/ANS.OR.B.005, system zarządzania ochroną w celu zapewnienia:

1) ochrony ich mienia i personelu, aby zapobiec bezprawnej ingerencji w zapewnianie służb;

2) ochrony otrzymanych bądź generowanych lub w inny sposób wykorzystywanych przez nie danych operacyjnych w celu ograniczenia dostępu do tych danych, tak aby miały go wyłącznie osoby upoważnione.

b) W systemie zarządzania ochroną określa się:

1) proces i procedury związane z oceną i ograniczaniem ryzyka w zakresie ochrony, monitorowaniem ochrony i jej poprawą, przeglądami ochrony i upowszechnianiem informacji o zdobytych doświadczeniach;

2) środki służące identyfikowaniu, monitorowaniu i wykrywaniu naruszeń w zakresie ochrony i powiadamianiu personelu o niebezpieczeństwie za pomocą odpowiednich ostrzeżeń;

3) środki służące kontrolowaniu skutków naruszeń w zakresie ochrony oraz określeniu działań naprawczych i procedur ograniczających, aby zapobiec ponownemu wystąpieniu naruszeń.

c) Instytucje zapewniające służby żeglugi powietrznej, instytucje zapewniające zarządzanie przepływem ruchu lotniczego oraz menedżer sieci zapewniają posiadanie przez członków ich personelu poświadczenia bezpieczeństwa osobowego, w stosownych przypadkach, i koordynują z odpowiednimi władzami cywilnymi i wojskowymi działania w celu zapewnienia ochrony swojego mienia, personelu i danych.

d) Aspektami związanymi z bezpieczeństwem informacji zarządza się zgodnie z pkt ATM/ANS.OR.B.005A.”.