Dziennik Urzędowy L 6

Unii Europejskiej

Wydanie polskie

Legislacja

Rocznik 60

11 stycznia 2017

Spis treści

PL

Akty, których tytuły wydrukowano zwykłą czcionką, odnoszą się do bieżącego zarządzania sprawami rolnictwa i generalnie zachowują ważność przez określony czas.

Tytuły wszystkich innych aktów poprzedza gwiazdka, a drukuje się je czcionką pogrubioną.

II

(Akty o charakterze nieustawodawczym)

UMOWY MIĘDZYNARODOWE

Informacja dotycząca wejścia w życie umowy między Unią Europejską a Republiką Kolumbii w sprawie zniesienia wiz krótkoterminowych

Umowa między Unią Europejską a Republiką Kolumbii w sprawie zniesienia wiz krótkoterminowych wejdzie w życie w dniu 1 grudnia 2016 r., przy czym procedura przewidziana w art. 8 ust. 1 umowy została zakończona w dniu 19 października 2016 r.

DECYZJA RADY (UE) 2017/43

z dnia 12 grudnia 2016 r.

w sprawie stanowiska, jakie należy przyjąć w imieniu Unii Europejskiej w Komitecie Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu utworzonym na mocy Układu o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony, w odniesieniu do aktualizacji załączników XXI-A do XXI-P dotyczących zbliżenia przepisów w dziedzinie zamówień publicznych

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 207 ust. 4 akapit pierwszy, w związku z art. 218 ust. 9,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) W art. 486 Układu o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony [1] (zwanego dalej „Układem"), przewidziano tymczasowe stosowanie Układu w części określonej przez Unię.

(2) W art. 1 decyzji Rady 2014/668/UE [2] określono postanowienia Układu, które mają być tymczasowo stosowane, a wśród nich postanowienia dotyczące zamówień publicznych oraz załącznik XXI do Układu. Postanowienia te są tymczasowo stosowane od dnia 1 stycznia 2016 r.

(3) Art. 153 Układu przewiduje, że Ukraina ma stopniowo zapewnić zgodność swoich przepisów dotyczących zamówień publicznych z odpowiednim dorobkiem prawnym Unii zgodnie z harmonogramem zawartym w załączniku XXI do Układu.

(4) Szereg aktów Unii wymienionych w załączniku XXI do Układu zostało zmienionych lub uchylonych od momentu parafowania Układu w dniu 30 marca 2012 r.

(5) Art. 149 Układu stanowi, że wartość progów dla zamówień publicznych przewidziana w załączniku XXI-P do Układu podlega regularnemu przeglądowi, począwszy od pierwszego parzystego roku po wejściu w życie Układu.

(6) Ponadto należy zmienić niektóre terminy, aby uwzględnić postępy osiągnięte przez Ukrainę w procesie zbliżania do unijnego dorobku prawnego.

(7) Należy zatem zaktualizować załącznik XXI, aby odzwierciedlić zmiany dotyczące unijnych aktów prawnych w nim wymienionych i dokonać korekty wartości progów dla zamówień publicznych przewidzianych w załączniku XXI-P do Układu.

(8) Art. 149 Układu stanowi, że korekty progów określonych w załączniku XXI-P do Układu dokonuje się w drodze decyzji Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu.

---

[1] Dz.U. L 161 z 29.5.2014, s. 3.

[2] Decyzja Rady 2014/668/UE z dnia 23 czerwca 2014 r. w sprawie podpisania, w imieniu Unii Europejskiej, oraz tymczasowego stosowania Układu o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony, w odniesieniu do jego tytułu III (z wyjątkiem postanowień dotyczących traktowania pracowników będących obywatelami państw trzecich legalnie zatrudnionych na terytorium drugiej Strony) oraz tytułów IV, V, VI i VII, jak również powiązanych załączników i protokołów (Dz.U. L 278 z 20.9.2014, s. 1).

(9) Art. 463 ust. 3 Układu stanowi, że Rada Stowarzyszenia jest uprawniona do aktualizacji i zmiany załączników do Układu.

(10) Art. 1 decyzji Rady Stowarzyszenia nr 3/2014 ([1]) przekazuje uprawnienia do aktualizacji i zmiany załączników do Układu związanych z handlem Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu, w tym załącznika XXI odnoszącego się do rozdziału 8 (Zamówienia publiczne) w tytule IV (Handel i zagadnienia związane z handlem).

(11) Należy zatem określić stanowisko, jakie powinno zostać zajęte w imieniu Unii w odniesieniu do aktualizacji załącznika XXI do Układu, która ma zostać przyjęta przez Komitet Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu.

(12) Art. 152 ust. 1 Układu stanowi, że Ukraina przedkłada Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu kompleksowy plan wdrożenia postanowień dotyczących zamówień publicznych, wraz z terminami i najważniejszymi etapami, które obejmują wszystkie reformy w zakresie zbliżenia przepisów i budowania zdolności instytucjonalnych. Harmonogram ten musi być zgodny z etapami i terminami przedstawionymi w załączniku XXI-A do Układu.

(13) Art. 152 ust. 3 precyzuje, że pozytywna opinia Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu jest potrzebna do uznania kompleksowego planu za dokument referencyjny dla procesu wdrożenia, to jest dla zbliżenia przepisów do przepisów dotyczących zamówień publicznych zawartych w unijnym dorobku prawnym.

(14) Należy zatem określić stanowisko, jakie powinno zostać zajęte w imieniu Unii w odniesieniu do pozytywnej opinii Komitetu Stowarzyszenia przyjętej w składzie rozstrzygającym kwestie dotyczące handlu w odniesieniu do przedstawionego przez Ukrainę kompleksowego planu,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Stanowisko, jakie ma zostać zajęte w imieniu Unii Europejskiej w Komitecie Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu ustanowionym na mocy art. 465 Układu o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony, w odniesieniu do aktualizacji załącznika XXI do Układu opiera się na projekcie decyzji tego komitetu dołączonym do niniejszej decyzji.

2. Przedstawiciele Unii w Komitecie Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu mogą uzgadniać niewielkie poprawki techniczne do projektu decyzji bez konieczności przyjmowania kolejnej decyzji przez Radę Unii Europejskiej.

Artykuł 2

Stanowisko, jakie ma zostać zajęte w imieniu Unii Europejskiej w Komitecie Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu ustanowionym na mocy art. 465 Układu w odniesieniu do pozytywnej opinii dotyczącej kompleksowego planu opiera się na projekcie decyzji tego komitetu, o której mowa w art. 1 ust. 1.

Artykuł 3

Decyzje Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu zostają opublikowane w *Dzienniku Urzędowym Unii Europejskiej* po ich przyjęciu.

([1]) Decyzja Rady Stowarzyszenia UE–Ukraina nr 3/2014 z dnia 15 grudnia 2014 r. w sprawie przekazania niektórych uprawnień Rady Stowarzyszenia Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu [2015/980] (Dz.U. L 158 z 24.6.2015, s. 4).

Artykuł 4

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w Brukseli dnia 12 grudnia 2016 r.

W imieniu Rady
F. MOGHERINI
Przewodniczący

PROJEKT

DECYZJA NR 1/2016 KOMITETU STOWARZYSZENIA UE-UKRAINA W SKŁADZIE ROZSTRZYGAJĄCYM KWESTIE DOTYCZĄCE HANDLU

z dnia …

w sprawie aktualizacji załącznika XXI do Układu o stowarzyszeniu oraz w sprawie pozytywnej opinii w odniesieniu do kompleksowego planu w dziedzinie zamówień publicznych

KOMITET STOWARZYSZENIA W SKŁADZIE ROZSTRZYGAJĄCYM KWESTIE DOTYCZĄCE HANDLU,

uwzględniając Układ o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony ([1]) (zwany dalej „Układem"), w szczególności jego art. 149, 153 i 463,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 486 Układu niektóre części Układu, w tym postanowienia dotyczące zamówień publicznych, stosuje się tymczasowo od dnia 1 stycznia 2016 r.

(2) Art. 149 Układu stanowi, że progi wartości dla zamówień publicznych przewidzianych w załączniku XXI-P podlegają regularnemu przeglądowi, począwszy od pierwszego parzystego roku po wejściu w życie Układu, a korekty tej dokonuje się w drodze decyzji Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu, o którym mowa w art. 465 ust. 4 Układu.

(3) Art. 153 Układu stanowi, że Ukraina ma stopniowo zapewnić zgodność swoich przepisów dotyczących zamówień publicznych z odpowiednim dorobkiem prawnym Unii zgodnie z harmonogramem zawartym w załączniku XXI do Układu.

(4) Od parafowania Układu w dniu 30 marca 2012 r. niektóre unijne akty prawne wymienione w załączniku XXI do Układu zostały przekształcone lub uchylone i zastąpione nowym aktem unijnym. W szczególności Unia przyjęła i notyfikowała Ukrainie następujące akty prawne:

a) dyrektywa Parlamentu Europejskiego i Rady 2014/23/UE ([2]);

b) dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE ([3]);

c) dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE ([4]).

(5) Wyżej wymienione dyrektywy wprowadziły zmiany progów wartości dla zamówień publicznych przewidzianych w załączniku XXI-P, które następnie zostały zmienione odpowiednio rozporządzeniami delegowanymi Komisji (UE) 2015/2170 ([5]), (UE) 2015/2171 ([6]), oraz (UE) 2015/2172 ([7]).

(6) Art. 463 ust. 3 Układu stanowi, że Rada Stowarzyszenia jest uprawniona do aktualizacji i zmiany załączników do Układu.

([1]) Dz.U. L 161 z 29.5.2014, s. 3.
([2]) Dyrektywa Parlamentu Europejskiego i Rady 2014/23/UE z dnia 26 lutego 2014 r. w sprawie udzielania koncesji (Dz.U. L 94 z 28.3.2014, s. 1).
([3]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).
([4]) Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz.U. L 94 z 28.3.2014, s. 243).
([5]) Rozporządzenie delegowane Komisji (UE) 2015/2170 z dnia 24 listopada 2015 r. zmieniające dyrektywę Parlamentu Europejskiego i Rady 2014/24/UE w odniesieniu do progów obowiązujących w zakresie procedur udzielania zamówień (Dz.U. L 307 z 25.11.2015, s. 5).
([6]) Rozporządzenie delegowane Komisji (UE) 2015/2171 z dnia 24 listopada 2015 r. zmieniające dyrektywę Parlamentu Europejskiego i Rady 2014/25/UE w odniesieniu do progów obowiązujących w zakresie procedur udzielania zamówień (Dz.U. L 307 z 25.11.2015, s. 7).
([7]) Rozporządzenie delegowane Komisji (UE) 2015/2172 z dnia 24 listopada 2015 r. zmieniające dyrektywę Parlamentu Europejskiego i Rady 2014/23/UE w odniesieniu do progów obowiązujących w zakresie procedur udzielania zamówień (Dz.U. L 307 z 25.11.2015, s. 9).

(7) Należy uaktualnić załącznik XXI do Układu, aby odzwierciedlał on zmiany dotyczące dorobku prawnego Unii wymienionego w tym załączniku, zgodnie z art. 149, 153 i 463 Układu.

(8) Nowy dorobek prawny Unii w dziedzinie zamówień publicznych ma nową strukturę. Należy uwzględnić tę nową strukturę w załączniku XXI. W interesie przejrzystości należy uaktualnić załącznik XXI w całości i zastąpić go załącznikiem o treści określonej w dodatku do niniejszej decyzji. Ponadto należy uwzględnić postępy osiągnięte przez Ukrainę w procesie zbliżenia przepisów do dorobku prawnego Unii.

(9) Art. 465 ust. 2 Układu stanowi, że Rada Stowarzyszenia może przekazać Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu swoje uprawnienia, w tym uprawnienie do podejmowania wiążących decyzji.

(10) Rada Stowarzyszenia UE-Ukraina decyzją nr 3/2014 ([1]) z dnia 15 grudnia 2014 r. upoważniła Komitet Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu do dokonania aktualizacji lub zmiany niektórych załączników dotyczących kwestii związanych z handlem.

(11) Art. 152 ust. 1 Układu stanowi, że Ukraina przedkłada Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu kompleksowy plan wdrożenia postanowień dotyczących zamówień publicznych, wraz z terminami i najważniejszymi etapami, które obejmują wszystkie reformy w zakresie zbliżenia przepisów do unijnego dorobku prawnego.

(12) Art. 152 ust. 3 precyzuje, że pozytywna opinia Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu jest potrzebna do tego, aby kompleksowy plan stał się dokumentem referencyjnym dla procesu wdrożenia, to jest dla zbliżenia ustawodawstwa do przepisów dotyczących zamówień publicznych zawartych w unijnym dorobku prawnym.

(13) W związku z tym Komitet Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu powinien wydać pozytywną opinię na temat kompleksowego planu,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Załącznik XXI do Układu o stowarzyszeniu między Unią Europejską i Europejską Wspólnotą Energii Atomowej oraz ich państwami członkowskimi, z jednej strony, a Ukrainą, z drugiej strony, zastępuje się załącznikiem o nowej treści, który jest dołączony do niniejszej decyzji.

Artykuł 2

Niniejszym pozytywnie opiniuje się kompleksowy plan zatwierdzony zarządzeniem Rady Ministrów Ukrainy z dnia 24 lutego 2016 r. (nr 175-p) przyjętym przez rząd Ukrainy dnia 24 lutego 2016 r.

Artykuł 3

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w …

W imieniu Komitetu Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu

Przewodniczący

([1]) Decyzja Rady Stowarzyszenia UE–Ukraina nr 3/2014 z dnia 15 grudnia 2014 r. w sprawie przekazania niektórych uprawnień Rady Stowarzyszenia Komitetowi Stowarzyszenia w składzie rozstrzygającym kwestie dotyczące handlu [2015/980] (Dz.U. L 158 z 24.6.2015, s. 4).

ZAŁĄCZNIK XXI-A DO ROZDZIAŁU 8

ORIENTACYJNY HARMONOGRAM REFORM INSTYTUCYJNYCH, ZBLIŻENIA PRZEPISÓW I PRZYZNANIA DOSTĘPU DO RYNKU

Etap		Orientacyjny harmonogram	Dostęp do rynku przyznany UE przez Ukrainę	Dostęp do rynku przyznany Ukrainie przez UE	
1.	Wykonanie art. 150 ust. 2 i art. 151 niniejszego Układu Uzgodnienie strategii reformy określonej w art. 152 niniejszego Układu	6 miesięcy po wejściu w życie niniejszego Układu	Dostawy dla instytucji administracji centralnej	Dostawy dla instytucji administracji centralnej	
2.	Zbliżenie przepisów i wdrożenie podstawowych elementów dyrektywy 2014/24/UE oraz dyrektywy Rady 89/665/EWG	3 lata po wejściu w życie niniejszego Układu	Dostawy dla władz państwowych, regionalnych i lokalnych oraz podmiotów prawa publicznego	Dostawy dla władz państwowych, regionalnych i lokalnych oraz podmiotów prawa publicznego	Załączniki XXI-B oraz XXI-C
3.	Zbliżenie przepisów i wdrożenie podstawowych elementów dyrektywy 2014/25/UE oraz dyrektywy 92/13/EWG	4 lata po wejściu w życie niniejszego Układu	Dostawy dla wszystkich zamawiających podmiotów w sektorze usług użyteczności publicznej	Dostawy dla wszystkich zamawiających podmiotów	Załączniki XXI-D oraz XXI-E
4.	Zbliżenie przepisów i wdrożenie innych elementów dyrektywy 2014/24/UE Zbliżenie przepisów i wdrożenie dyrektywy 2014/23/UE	6 lat po wejściu w życie niniejszego Układu	Zamówienia na roboty budowlane i usługi oraz koncesje dla wszystkich instytucji zamawiających	Zamówienia na roboty budowlane i usługi oraz koncesje dla wszystkich instytucji zamawiających	Załączniki XXI-F, XXI-G oraz XXI-H
5.	Zbliżenie przepisów i wdrożenie innych elementów dyrektywy 2014/25/UE	8 lat po wejściu w życie niniejszego Układu	Zamówienia na roboty budowlane i usługi dla wszystkich zamawiających podmiotów w sektorze usług użyteczności publicznej	Zamówienia na roboty budowlane i usługi dla wszystkich zamawiających podmiotów w sektorze usług użyteczności publicznej	Załączniki XXI–I oraz XXI-J

ZAŁĄCZNIK XXI-B DO ROZDZIAŁU 8

PODSTAWOWE ELEMENTY DYREKTYWY 2014/24/UE

z dnia 26 lutego 2014 r. w sprawie zamówień publicznych

(Etap 2)

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Zakres stosowania i definicje

Sekcja 1	Przedmiot i definicje
Artykuł 1	Przedmiot i zakres stosowania ust. 1, 2, 5 i 6
Artykuł 2	Definicje ust. 1 pkt 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 18, 19, 20, 22, 23, 24
Artykuł 3	Zamówienia mieszane
Sekcja 2	Progi
Artykuł 4	Kwoty progowe
Artykuł 5	Metody obliczania szacunkowej wartości zamówienia
Sekcja 3	Wyłączenia
Artykuł 7	Zamówienia w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych
Artykuł 8	Szczególne wyłączenia w dziedzinie łączności elektronicznej
Artykuł 9	Zamówienia publiczne udzielane i konkursy organizowane zgodnie z przepisami międzynarodowymi
Artykuł 10	Wyłączenia szczególne dotyczące zamówień na usługi
Artykuł 11	Zamówienia na usługi udzielane na podstawie prawa wyłącznego
Artykuł 12	Zamówienia publiczne między podmiotami sektora publicznego
Sekcja 4	Sytuacje szczególne
Podsekcja 1:	Zamówienia subsydiowane oraz usługi badawcze i rozwojowe
Artykuł 13	Zamówienia subsydiowane przez instytucje zamawiające
Artykuł 14	Usługi badawcze i rozwojowe
Podsekcja 2:	Zamówienia obejmujące aspekty obronności lub bezpieczeństwa
Artykuł 15	Obronność i bezpieczeństwo
Artykuł 16	Zamówienia mieszane obejmujące aspekty obronności lub bezpieczeństwa
Artykuł 17	Zamówienia publiczne i konkursy obejmujące aspekty obronności lub bezpieczeństwa, udzielane lub organizowane na mocy przepisów międzynarodowych

ROZDZIAŁ II

Przepisy ogólne

Artykuł 18	Zasady udzielania zamówień
Artykuł 19	Wykonawcy
Artykuł 21	Poufność
Artykuł 22	Zasady mające zastosowanie do komunikacji ust. 2–6

ZAŁĄCZNIK XXI-C DO ROZDZIAŁU 8

PODSTAWOWE ELEMENTY DYREKTYWY 89/665/EWG

z dnia 21 grudnia 1989 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do stosowania procedur odwoławczych w zakresie udzielania zamówień publicznych na dostawy i roboty budowlane (dyrektywa 89/665/EWG)

zmienionej dyrektywą 2007/66/WE Parlamentu Europejskiego i Rady z dnia 11 grudnia 2007 r. zmieniającą dyrektywy Rady 89/665/EWG i 92/13/EWG w zakresie poprawy skuteczności procedur odwoławczych w dziedzinie udzielania zamówień publicznych (dyrektywa 2007/66/WE) oraz dyrektywą Parlamentu Europejskiego i Rady 2014/23/UE z dnia 26 lutego 2014 r. w sprawie udzielania koncesji (dyrektywa 2014/23/UE)

(Etap 2)

Artykuł 1	Zakres stosowania i dostępność procedur odwoławczych
Artykuł 2	Wymogi dotyczące procedur odwoławczych
Artykuł 2a	Okres zawieszenia typu *standstill*
Artykuł 2b	Wyjątki od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. b)
Artykuł 2c	Terminy na wniesienie odwołania
Artykuł 2d	Nieskuteczność
	ust. 1 lit. b)
	ust. 2 i 3
Artykuł 2e	Naruszenia niniejszej dyrektywy i inne kary
Artykuł 2f	Terminy

ZAŁĄCZNIK XXI-D DO ROZDZIAŁU 8

PODSTAWOWE ELEMENTY DYREKTYWY 2014/25/UE

z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych

(Etap 3)

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Przedmiot i definicje

Artykuł 1	Przedmiot i zakres stosowania ust. 1, 2, 5 i 6
Artykuł 2	Definicje pkt 1–9, 13–16 i 18–20
Artykuł 3	Instytucje zamawiające (ust. 1 i 4)
Artykuł 4	Podmioty zamawiające ust. 1-3
Artykuł 5	Zamówienia mieszane obejmujące taki sam rodzaj działalności
Artykuł 6	Zamówienia obejmujące kilka rodzajów działalności

ROZDZIAŁ II

Rodzaje działalności

Artykuł 7	Przepisy wspólne
Artykuł 8	Gaz i energia cieplna
Artykuł 9	Energia elektryczna
Artykuł 10	Gospodarka wodna
Artykuł 11	Usługi transportowe
Artykuł 12	Porty i porty lotnicze
Artykuł 13	Usługi pocztowe
Artykuł 14	Wydobycie ropy naftowej i gazu oraz poszukiwanie lub wydobycie węgla lub innych paliw stałych

ROZDZIAŁ III

Zakres przedmiotowy

Sekcja 1	Progi
Artykuł 15	Kwoty progowe
Artykuł 16	Metody obliczania szacunkowej wartości zamówienia ust. 1–4 i 7–14
Sekcja 2	Zamówienia i konkursy wyłączone: przepisy szczególne dotyczące zamówień obejmujących aspekty obronności i bezpieczeństwa
Podsekcja 1:	Wyłączenia mające zastosowanie do wszystkich podmiotów zamawiających oraz szczególne wyłączenia dotyczące sektorów gospodarki wodnej i energetyki
Artykuł 18	Zamówienia udzielane na potrzeby odsprzedaży lub dzierżawy osobom trzecim ust. 1
Artykuł 19	Zamówienia udzielane i konkursy organizowane w innym celu niż wykonywanie jednego z rodzajów działalności objętych niniejszą dyrektywą lub w celu wykonywania takiej działalności w państwie trzecim ust. 1
Artykuł 20	Zamówienia udzielane i konkursy organizowane zgodnie z przepisami międzynarodowymi

ZAŁĄCZNIK XXI-E DO ROZDZIAŁU 8

PODSTAWOWE ELEMENTY DYREKTYWY RADY 92/13/EWG

z dnia 25 lutego 1992 r. koordynującej przepisy ustawowe, wykonawcze i administracyjne odnoszące się do stosowania przepisów wspólnotowych w procedurach zamówień publicznych podmiotów działających w sektorach gospodarki wodnej, energetyki, transportu i telekomunikacji (dyrektywa 92/13/EWG)

zmienionej dyrektywą 2007/66/WE oraz dyrektywą 2014/23/UE

(Etap 3)

Artykuł 1	Zakres stosowania i dostępność procedur odwoławczych
Artykuł 2	Wymogi dotyczące procedur
Artykuł 2a	Okres zawieszenia typu *standstill*
Artykuł 2b	Odstępstwa od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. b)
Artykuł 2c	Terminy na wniesienia odwołań
Artykuł 2d	Nieskuteczność
	ust. 1 lit. b), 2 i 3
Artykuł 2e	Naruszenia niniejszej dyrektywy i inne kary
Artykuł 2f	Terminy

ZAŁĄCZNIK XXI-F DO ROZDZIAŁU 8

I. INNE NIEOBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/24/UE

(Etap 4)

Elementy dyrektywy 2014/24/UE wymienione w niniejszym załączniku nie są obowiązkowe, są jednak zalecane w ramach zbliżania przepisów. Ukraina może dokonać zbliżenia tych elementów w terminie określonym w załączniku XXI-B.

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Zakres stosowania i definicje

Sekcja 1	Przedmiot i definicje
Artykuł 2	Definicje (ust. 1 pkt 14 i 16)
Artykuł 20	Zamówienia zastrzeżone

TYTUŁ II

Przepisy dotyczące zamówień publicznych

ROZDZIAŁ II

Techniki i instrumenty w zakresie zamówień elektronicznych i zamówień zagregowanych

Artykuł 37	Scentralizowane działania zakupowe i centralne jednostki zakupujące

ROZDZIAŁ III

Przeprowadzenie postępowania

Sekcja 3	Wybór uczestników oraz udzielenie zamówienia
Artykuł 64	Urzędowe wykazy zatwierdzonych wykonawców oraz certyfikacja przez jednostki prawa publicznego lub prywatnego

TYTUŁ III

Szczególne reżimy udzielania zamówień

ROZDZIAŁ I

Artykuł 77	Zamówienia zastrzeżone w odniesieniu do określonych usług

II. NIEOBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/23/UE

(Etap 4)

Elementy dyrektywy 2014/23/UE wymienione w niniejszym załączniku nie są obowiązkowe, są jednak zalecane w ramach zbliżania przepisów. Ukraina może dokonać zbliżenia tych elementów w terminie określonym w załączniku XXI-B.

TYTUŁ I

Przedmiot, zakres stosowania, zasady ogólne i definicje

ROZDZIAŁ I

Zakres stosowania, zasady ogólne i definicje

Sekcja IV	Sytuacje szczególne
Artykuł 24	Koncesje zastrzeżone

ZAŁĄCZNIK XXI-G DO ROZDZIAŁU 8

I. INNE OBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/24/UE

(ETAP 4)

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Zakres stosowania i definicje

Sekcja 1	Przedmiot i definicje
Artykuł 2	Definicje (ust. 1 pkt 21)
Artykuł 22	Zasady mające zastosowanie do komunikacji ust. 1

TYTUŁ II

Przepisy dotyczące zamówień publicznych

ROZDZIAŁ I

Procedury

Artykuł 26	Wybór procedury ust. 3, druga alternatywa w ust. 4
Artykuł 30	Dialog konkurencyjny
Artykuł 31	Partnerstwo innowacyjne

ROZDZIAŁ II

Techniki i instrumenty w zakresie zamówień elektronicznych i zamówień zagregowanych

Artykuł 33	Umowy ramowe
Artykuł 34	Dynamiczne systemy zakupów
Artykuł 35	Aukcje elektroniczne
Artykuł 36	Katalogi elektroniczne
Artykuł 38	Okazjonalne wspólne udzielanie zamówień

ROZDZIAŁ III

Przeprowadzenie postępowania

Sekcja 2	Publikacja i przejrzystość
Artykuł 50	Ogłoszenie o udzieleniu zamówienia ust. 2 i 3

TYTUŁ III

Szczególne reżimy udzielania zamówień

ROZDZIAŁ II

Przepisy dotyczące konkursów

Artykuł 78	Zakres stosowania
Artykuł 79	Ogłoszenia
Artykuł 80	Reguły dotyczące organizacji konkursów i kwalifikacji uczestników
Artykuł 81	Skład sądu konkursowego
Artykuł 82	Decyzje sądu konkursowego

ZAŁĄCZNIKI

ZAŁĄCZNIK V	INFORMACJE, JAKIE NALEŻY ZAMIEŚCIĆ W OGŁOSZENIU
	Część E: INFORMACJE, JAKIE NALEŻY ZAMIEŚCIĆ W OGŁOSZENIU O KONKURSIE (o którym mowa w art. 79 ust. 1)
	Część F: INFORMACJE, JAKIE NALEŻY ZAMIEŚCIĆ W OGŁOSZENIU O WYNIKACH KONKURSU (o którym mowa w art. 79 ust. 2)
ZAŁĄCZNIK VI:	INFORMACJE, JAKIE NALEŻY ZAMIEŚCIĆ W DOKUMENTACH ZAMÓWIENIA DOTYCZĄCYCH AUKCJI ELEKTRONICZNEJ (ART. 35 UST. 4)

II. OBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/23/UE

(Etap 4)

TYTUŁ I

Przedmiot, zakres stosowania, zasady ogólne i definicje

ROZDZIAŁ I

Zakres stosowania, zasady ogólne i definicje

Sekcja I	Przedmiot, zakres stosowania, zasady ogólne i próg
Artykuł 1	Przedmiot i zakres stosowania ust. 1, 2 i 4
Artykuł 2	Zasada swobodnego administrowania przez organy władzy publicznej
Artykuł 3	Zasada równego traktowania, niedyskryminacji i przejrzystości
Artykuł 4	Swoboda określania usług świadczonych w ogólnym interesie gospodarczym
Artykuł 5	Definicje
Artykuł 6	Instytucje zamawiające ust. 1 i 4
Artykuł 7	Podmioty zamawiające
Artykuł 8:	Próg i metody obliczania szacunkowej wartości koncesji
Sekcja II	Wyłączenia
Artykuł 10	Wyłączenia dotyczące koncesji udzielanych przez instytucje zamawiające i podmioty zamawiające
Artykuł 11	Wyłączenia szczególne w dziedzinie łączności elektronicznej
Artykuł 12	Wyłączenia szczególne w sektorze wodnym
Artykuł 13	Koncesje udzielane przedsiębiorstwu powiązanemu
Artykuł 14	Koncesje udzielane przedsięwzięciu typu joint venture lub podmiotowi zamawiającemu wchodzącemu w skład przedsięwzięcia typu joint venture
Artykuł 17	Koncesje między podmiotami w sektorze publicznym
Sekcja III	Przepisy ogólne
Artykuł 18	Okres obowiązywania koncesji
Artykuł 19	Usługi społeczne i inne szczególne usługi
Artykuł 20	Koncesje mieszane
Artykuł 21	Zamówienia mieszane obejmujące aspekty obronności lub bezpieczeństwa
Artykuł 22	Koncesje obejmujące zarówno rodzaje działalności, o których mowa w załączniku II, jak i inne rodzaje działalności
Artykuł 23	Koncesje dotyczące rodzajów działalności, o których mowa w załączniku II, i rodzajów działalności obejmujących aspekty obronności lub bezpieczeństwa
Artykuł 25	Usługi badawcze i rozwojowe

ZAŁĄCZNIK XXI-H DO ROZDZIAŁU 8

INNE ELEMENTY DYREKTYWY 89/665/EWG

zmienionej dyrektywą 2007/66/WE oraz dyrektywą 2014/23/UE

(Etap 4)

Artykuł 2b	Odstępstwa od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. c)
Artykuł 2d	Nieskuteczność
	Artykuł 2d ust. 1 lit. c)
	ust. 5

ZAŁĄCZNIK XXI–I DO ROZDZIAŁU 8

(Etap 5)

I. INNE OBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/25/UE

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Przedmiot i definicje

Artykuł 2	Definicje pkt 17

ROZDZIAŁ III

Zakres przedmiotowy

Sekcja 1	Progi
Artykuł 16	Metody obliczania szacunkowej wartości zamówienia ust. 5, 6

TYTUŁ II

Przepisy mające zastosowanie do zamówień

ROZDZIAŁ I

Procedury

Artykuł 44	Wybór procedury ust. 3
Artykuł 48	Dialog konkurencyjny
Artykuł 49	Partnerstwo innowacyjne
Artykuł 50	Stosowanie procedury negocjacyjnej bez uprzedniego zaproszenia do ubiegania się o zamówienie lit. j)

ROZDZIAŁ II

Techniki i instrumenty w zakresie zamówień elektronicznych i zamówień zagregowanych

Artykuł 51	Umowy ramowe
Artykuł 52	Dynamiczne systemy zakupów
Artykuł 53	Aukcje elektroniczne
Artykuł 54	Katalogi elektroniczne
Artykuł 56	Okazjonalne wspólne udzielanie zamówień

ROZDZIAŁ III

Przeprowadzenie postępowania

Sekcja 2	Publikacja i przejrzystość
Artykuł 70	Ogłoszenie o udzieleniu zamówienia ust. 2
Sekcja 3	Wybór uczestników oraz udzielenie zamówienia
Podsekcja 1:	Systemy kwalifikowania oraz kwalifikacja podmiotowa
Artykuł 77	Systemy kwalifikowania
Artykuł 79	Poleganie na zdolności innych podmiotów ust. 1

TYTUŁ III

Szczególne reżimy udzielania zamówień

ROZDZIAŁ II

Przepisy dotyczące konkursów

Artykuł 95	Zakres stosowania
Artykuł 96	Ogłoszenia
Artykuł 97	Przepisy dotyczące organizacji konkursów, kwalifikacji uczestników oraz sądu konkursowego
Artykuł 98	Decyzje sądu konkursowego

ZAŁĄCZNIKI

ZAŁĄCZNIK VII	Informacje, jakie należy zamieścić w dokumentach zamówienia dotyczących aukcji elektronicznej (art. 53 ust. 4)
ZAŁĄCZNIK XIX	Informacje, jakie należy zamieścić w ogłoszeniu o konkursie (zgodnie z art. 96 ust. 1)
ZAŁĄCZNIK XX	Informacje, jakie należy zamieścić w ogłoszeniu o konkursie (zgodnie z art. 96 ust. 1)

II. INNE NIEOBOWIĄZKOWE ELEMENTY DYREKTYWY 2014/25/UE

Elementy dyrektywy 2014/25/UE wymienione w niniejszym załączniku nie są obowiązkowe, są jednak zalecane w ramach zbliżania przepisów. Ukraina może dokonać zbliżenia tych elementów w terminie określonym w załączniku XXI-B.

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Przedmiot i definicje

Artykuł 2	Definicje pkt 10–12

ROZDZIAŁ IV

Zasady ogólne

Artykuł 38	Zamówienia zastrzeżone

TYTUŁ II

Przepisy mające zastosowanie do zamówień

ROZDZIAŁ I

Procedury

Artykuł 55	Scentralizowane działania zakupowe i centralne jednostki zakupujące

TYTUŁ III

Szczególne reżimy udzielania zamówień

ROZDZIAŁ I

Usługi społeczne i inne szczególne usługi

Artykuł 94	Zamówienia zastrzeżone w odniesieniu do określonych usług

ZAŁĄCZNIK XXI-J DO ROZDZIAŁU 8

INNE ELEMENTY DYREKTYWY 92/13/EWG

zmienionej dyrektywą 2007/66/WE oraz dyrektywą 2014/23/UE

(Etap 5)

Artykuł 2b	Odstępstwa od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. c)
Artykuł 2d	Nieskuteczność
	Artykuł 2d ust. 1 lit. c)
	ust. 5

ZAŁĄCZNIK XXI-K DO ROZDZIAŁU 8

I. PRZEPISY DYREKTYWY 2014/24/UE POZA ZAKRESEM ZBLIŻENIA

Elementy dyrektywy 2014/24/UE wymienione w niniejszym załączniku nie są objęte procesem zbliżenia.

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Zakres stosowania i definicje

Sekcja 1	Przedmiot i definicje
Artykuł 1	Przedmiot i zakres stosowania ust. 3 i 4
Artykuł 2	Definicje ust. 2
Sekcja 2	Progi
Artykuł 6	Korekta progów i wykazu instytucji administracji centralnej

TYTUŁ II

Przepisy dotyczące zamówień publicznych

ROZDZIAŁ I

Procedury

Artykuł 25	Warunki dotyczące Porozumienia GPA i innych umów międzynarodowych

ROZDZIAŁ II

Techniki i instrumenty w zakresie zamówień elektronicznych i zamówień zagregowanych

Artykuł 39	Zamówienia, w których biorą udział instytucje zamawiające z różnych państw członkowskich

ROZDZIAŁ III

Przeprowadzenie postępowania

Sekcja 1	Przygotowanie
Artykuł 44	Raporty z testów, certyfikacja i inne środki dowodowe ust. 3
Sekcja 2	Publikacja i przejrzystość
Artykuł 51	Forma i sposób publikacji ogłoszeń ust. 1 akapit drugi, ust. 2, 3, 4, ust. 5 akapit drugi, ust. 6
Artykuł 52	Publikacja na poziomie krajowym
Sekcja 3	Wybór uczestników oraz udzielenie zamówienia
Artykuł 61	Internetowe repozytorium zaświadczeń (e-Certis)
Artykuł 62	Normy zapewniania jakości i normy zarządzania środowiskowego ust. 3
Artykuł 68	Rachunek kosztów cyklu życia ust. 3
Artykuł 69	Rażąco tanie oferty ust. 5

TYTUŁ IV

Ład administracyjno-regulacyjny

Artykuł 83	Egzekwowanie przepisów
Artykuł 84	Indywidualne sprawozdania dotyczące postępowań o udzielenie zamówienia
Artykuł 85	Sprawozdania krajowe i informacje statystyczne
Artykuł 86	Współpraca administracyjna

II. PRZEPISY DYREKTYWY 2014/23/UE POZA ZAKRESEM ZBLIŻENIA

Elementy dyrektywy 2014/23/UE wymienione w niniejszym załączniku nie są objęte procesem zbliżenia.

ZAŁĄCZNIK XXI-L DO ROZDZIAŁU 8

PRZEPISY DYREKTYWY 2014/25/UE POZA ZAKRESEM ZBLIŻENIA

Elementy wymienione w niniejszym załączniku nie są objęte procesem zbliżenia.

TYTUŁ I

Zakres stosowania, definicje i zasady ogólne

ROZDZIAŁ I

Przedmiot i definicje

Artykuł 1	Przedmiot i zakres stosowania: ust. 3 i 4
Artykuł 3	Instytucje zamawiające ust. 2 i 3
Artykuł 4	Podmioty zamawiające ust. 4

ROZDZIAŁ III

Zakres przedmiotowy

Sekcja 1	Progi
Artykuł 17	Korekta progów
Sekcja 2	Zamówienia i konkursy wyłączone: przepisy szczególne dotyczące zamówień obejmujących aspekty obronności i bezpieczeństwa
Podsekcja 1:	Wyłączenia mające zastosowanie do wszystkich podmiotów zamawiających oraz szczególne wyłączenia dotyczące sektorów gospodarki wodnej i energetyki
Artykuł 18	Zamówienia udzielane na potrzeby odsprzedaży lub dzierżawy osobom trzecim ust. 2
Artykuł 19	Zamówienia udzielane i konkursy organizowane w innym celu niż wykonywanie jednego z rodzajów działalności objętych niniejszą dyrektywą lub w celu wykonywania takiej działalności w państwie trzecim ust. 2
Podsekcja 3:	Stosunki szczególne (współpraca, przedsiębiorstwa powiązane oraz przedsięwzięcia typu joint venture)
Artykuł 31	Przekazywanie informacji
Podsekcja 4:	Sytuacje szczególne
Artykuł 33	Zamówienia podlegające szczególnym ustaleniom
Podsekcja 5:	Rodzaje działalności bezpośrednio podlegające konkurencji oraz dotyczące ich przepisy proceduralne
Artykuł 34	Rodzaje działalności bezpośrednio podlegające konkurencji
Artykuł 35	Procedura do celów ustalenia, czy zastosowanie ma art. 34

TYTUŁ II

Przepisy mające zastosowanie do zamówień

ROZDZIAŁ I

Procedury

Artykuł 43	Warunki dotyczące Porozumienia GPA i innych umów międzynarodowych

ROZDZIAŁ II

Techniki i instrumenty w zakresie zamówień elektronicznych i zagregowanych

Artykuł 57	Zamówienia, w których biorą udział podmioty zamawiające z różnych państw członkowskich

ZAŁĄCZNIK XXI-M DO ROZDZIAŁU 8

PRZEPISY DYREKTYWY 89/665/EWG ZMIENIONEJ DYREKTYWĄ 2007/66/WE I DYREKTYWĄ 2014/23/UE POZA ZAKRESEM ZBLIŻENIA

Elementy wymienione w niniejszym załączniku nie są objęte procesem zbliżenia.

Artykuł 2b	Odstępstwa od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. a)
Artykuł 2d	Nieskuteczność
	Artykuł 2d ust. 1 lit. a)
	ust. 4
Artykuł 3	Mechanizm korygujący
Artykuł 3a	Treść ogłoszenia o dobrowolnej przejrzystości *ex ante*
Artykuł 3b	Procedura komitetu
Artykuł 4	Wykonanie
Artykuł 4a	Przegląd

ZAŁĄCZNIK XXI-N DO ROZDZIAŁU 8

PRZEPISY DYREKTYWY 92/13/EWG ZMIENIONEJ DYREKTYWĄ 2007/66/WE I DYREKTYWĄ 2014/23/UE POZA ZAKRESEM ZBLIŻENIA

Elementy wymienione w niniejszym załączniku nie są objęte procesem zbliżenia.

Artykuł 2b	Odstępstwa od okresu zawieszenia typu *standstill*
	Artykuł 2b akapit pierwszy lit. a)
Artykuł 2d	Nieskuteczność
	Artykuł 2d ust. 1 lit. a)
	ust. 4
Artykuł 3a	Treść ogłoszenia o dobrowolnej przejrzystości *ex ante*
Artykuł 3b	Procedura komitetu
Artykuł 8	Mechanizm korygujący
Artykuł 12	Wykonanie
Artykuł 12a	Przegląd

ZAŁĄCZNIK XXI-O DO ROZDZIAŁU 8

UKRAINA ORIENTACYJNY WYKAZ ZAGADNIEŃ OBJĘTYCH WSPÓŁPRACĄ

1. szkolenie, na Ukrainie i w państwach UE, urzędników ukraińskich z organów rządowych zaangażowanych w zamówienia publiczne;

2. szkolenie dostawców zainteresowanych uczestnictwem w zamówieniach publicznych;

3. wymiana informacji i doświadczeń na temat najlepszych praktyk oraz zasad regulacyjnych w obszarze zamówień publicznych;

4. zwiększenie funkcjonalności strony internetowej poświęconej zamówieniom publicznym oraz utworzenie systemu monitorowania zamówień publicznych;

5. konsultacje i pomoc metodologiczna oferowana przez Stronę UE w zakresie stosowania nowoczesnych technologii elektronicznych w obszarze zamówień publicznych;

6. wzmocnienie organów odpowiedzialnych za zapewnienie spójnej polityki we wszystkich obszarach związanych z zamówieniami publicznymi oraz za niezależną i bezstronną weryfikację decyzji instytucji zmawiających. (zob. art. 150 ust. 2 niniejszego Układu)

ZAŁĄCZNIK XXI-P DO ROZDZIAŁU 8

PROGI

1. Wartość progów wymienionych w art. 149 ust. 3 niniejszego Układu dla obu Stron wynosi:

   a) 135 000 EUR dla zamówień publicznych na dostawy i usługi udzielanych przez instytucje administracji centralnej lub konkursów organizowanych przez te instytucje;

   b) 209 000 EUR w przypadku zamówień publicznych na dostawy i usługi nie ujętych w lit. a);

   c) 5 225 000 EUR dla zamówień publicznych na roboty budowlane;

   d) 5 225 000 EUR dla zamówień na roboty budowlane w sektorze użyteczności publicznej;

   e) 5 225 000 EUR dla koncesji;

   f) 418 000 EUR dla zamówień na dostawy i usługi w sektorze użyteczności publicznej;

   g) 750 000 EUR dla zamówień publicznych na usługi społeczne i inne szczególne usługi;

   h) 1 000 000 EUR dla zamówień publicznych na usługi społeczne i inne szczególne usługi w sektorze użyteczności publicznej.

2. Progi wartości, o których mowa w ust. 1, dostosowuje się w celu odzwierciedlenia progów mających zastosowanie na podstawie unijnych dyrektyw w chwili wejścia w życie niniejszego Układu.

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2017/44

z dnia 10 stycznia 2017 r.

zmieniające rozporządzenie Rady (WE) nr 1210/2003 dotyczące niektórych szczególnych ograniczeń w stosunkach gospodarczych i finansowych z Irakiem

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (WE) nr 1210/2003 z dnia 7 lipca 2003 r. dotyczące niektórych szczególnych ograniczeń w stosunkach gospodarczych i finansowych z Irakiem oraz uchylające rozporządzenie (WE) nr 2465/96 ([1]), w szczególności jego art. 11 lit. b),

a także mając na uwadze, co następuje:

(1) Załącznik III do rozporządzenia (WE) nr 1210/2003 zawiera wykaz instytucji publicznych, korporacji i agend oraz osób fizycznych i prawnych, organów i podmiotów byłego rządu Iraku objętych zamrożeniem funduszy i zasobów gospodarczych znajdujących się poza Irakiem w dniu 22 maja 2003 r. zgodnie z tym rozporządzeniem.

(2) Dnia 28 grudnia 2016 r. Komitet ds. Sankcji Rady Bezpieczeństwa ONZ podjął decyzję o wykreśleniu 2 pozycji z wykazu osób lub podmiotów, względem których należy stosować zamrożenie funduszy i zasobów gospodarczych.

(3) Należy zatem odpowiednio zmienić załącznik III do rozporządzenia (WE) nr 1210/2003,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W załączniku III do rozporządzenia (WE) nr 1210/2003 wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

Artykuł 2

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

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

Sporządzono w Brukseli dnia 10 stycznia 2017 r.

W imieniu Komisji,

za Przewodniczącego,

p.o. Szefa Służby ds. Instrumentów Polityki Zagranicznej

([1]) Dz.U. L 169 z 8.7.2003, s. 6.

ZAŁĄCZNIK

W załączniku III do rozporządzenia Rady (WE) nr 1210/2003 skreśla się wpisy w brzmieniu:

„78. MEDICAL CITY ESTABLISHMENT. Adres: Baghdad, Iraq.

115. STATE COMPANY FOR DRUGS AND MEDICAL APPLIANCES (alias (a) GENERAL ESTABLISHMENT FOR DRUGS & MEDICAL APPLICANCES, (b) KIMADIA). Adres: Mansour City, P.O. Box 6138, Baghdad, Iraq.”.

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2017/45

z dnia 10 stycznia 2017 r.

ustanawiające standardowe wartości w przywozie dla ustalania ceny wejścia niektórych owoców i warzyw

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1308/2013 z dnia 17 grudnia 2013 r. ustanawiające wspólną organizację rynków produktów rolnych oraz uchylające rozporządzenia Rady (EWG) nr 922/72, (EWG) nr 234/79, (WE) nr 1037/2001 i (WE) nr 1234/2007 ([1]),

uwzględniając rozporządzenie wykonawcze Komisji (UE) nr 543/2011 z dnia 7 czerwca 2011 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1234/2007 w odniesieniu do sektorów owoców i warzyw oraz przetworzonych owoców i warzyw ([2]), w szczególności jego art. 136 ust. 1,

a także mając na uwadze, co następuje:

(1) Rozporządzenie wykonawcze (UE) nr 543/2011 przewiduje – zgodnie z wynikami wielostronnych negocjacji handlowych Rundy Urugwajskiej – kryteria, na których podstawie Komisja ustala standardowe wartości dla przywozu z państw trzecich, w odniesieniu do produktów i okresów określonych w części A załącznika XVI do wspomnianego rozporządzenia.

(2) Standardowa wartość w przywozie jest obliczana każdego dnia roboczego, zgodnie z art. 136 ust. 1 rozporządzenia wykonawczego (UE) nr 543/2011, przy uwzględnieniu podlegających zmianom danych dziennych. Niniejsze rozporządzenie powinno zatem wejść w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Standardowe wartości celne w przywozie, o których mowa w art. 136 rozporządzenia wykonawczego (UE) nr 543/2011, są ustalone w załączniku do niniejszego rozporządzenia.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

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

Sporządzono w Brukseli dnia 10 stycznia 2017 r.

W imieniu Komisji,

za Przewodniczącego,

Jerzy PLEWA

Dyrektor Generalny

Dyrekcja Generalna ds. Rolnictwa i Rozwoju Obszarów Wiejskich

([1]) Dz.U. L 347 z 20.12.2013, s. 671.
([2]) Dz.U. L 157 z 15.6.2011, s. 1.

ZAŁĄCZNIK

Standardowe wartości w przywozie dla ustalania ceny wejścia niektórych owoców i warzyw

(EUR/100 kg)

Kod CN	Kod państw trzecich (1)	Standardowa wartość w przywozie
0702 00 00	IL	261,0
	MA	110,4
	SN	204,0
	TR	102,4
	ZZ	169,5
0707 00 05	MA	85,5
	TR	213,8
	ZZ	149,7
0709 91 00	EG	144,1
	ZZ	144,1
0709 93 10	MA	238,8
	TR	213,8
	ZZ	226,3
0805 10 20	EG	42,5
	IL	126,4
	MA	55,6
	TR	71,5
	ZZ	74,0
0805 20 10	IL	166,4
	MA	85,6
	ZZ	126,0
0805 20 30, 0805 20 50, 0805 20 70, 0805 20 90	IL	136,2
	JM	125,6
	TR	96,4
	ZZ	119,4
0805 50 10	TR	71,8
	ZZ	71,8
0808 10 80	CN	144,5
	US	105,5
	ZZ	125,0
0808 30 90	CL	282,6
	CN	99,5
	TR	133,1
	ZZ	171,7

(1) Nomenklatura krajów ustalona w rozporządzeniu Komisji (UE) nr 1106/2012 z dnia 27 listopada 2012 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 471/2009 w sprawie statystyk Wspólnoty dotyczących handlu zagranicznego z państwami trzecimi, w odniesieniu do aktualizacji nazewnictwa państw i terytoriów (Dz.U. L 328 z 28.11.2012, s. 7). Kod „ZZ" odpowiada „innym pochodzeniom".

DECYZJE

DECYZJA KOMISJI (UE, Euratom) 2017/46

z dnia 10 stycznia 2017 r.

w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 249,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej,

a także mając na uwadze, co następuje:

(1) Systemy teleinformatyczne Komisji są nieodłącznie związane z funkcjonowaniem Komisji, a incydenty związane z bezpieczeństwem systemów IT mogą mieć poważny wpływ na działania podejmowane przez Komisję, jak również na osoby trzecie, w tym osoby fizyczne, przedsiębiorstwa i państwa członkowskie.

(2) Istnieje wiele zagrożeń, które mogą zaszkodzić poufności, integralności lub dostępności systemów teleinformatycznych Komisji oraz informacjom przechowywanym w tych systemach. Zagrożenia te obejmują wypadki, błędy, zamierzone ataki oraz zjawiska naturalne i należy je uznać za rodzaje ryzyka operacyjnego.

(3) Systemom teleinformatycznym należy zapewnić poziom ochrony proporcjonalny do prawdopodobieństwa, wpływu i charakteru rodzajów ryzyka, na które są narażone.

(4) Bezpieczeństwo IT w Komisji powinno zapewnić, by systemy teleinformatyczne Komisji chroniły informacje, które przetwarzają, i funkcjonowały stosownie do potrzeb, gdy zachodzi potrzeba, oraz pod kontrolą uprawnionych użytkowników.

(5) Politykę w zakresie bezpieczeństwa IT Komisji należy wdrażać w sposób spójny z polityką dotyczącą bezpieczeństwa w Komisji.

(6) Dyrekcja ds. Bezpieczeństwa Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa ponosi ogólną odpowiedzialność za bezpieczeństwo w Komisji z upoważnienia członka Komisji odpowiedzialnego za bezpieczeństwo i na jego odpowiedzialność.

(7) Podejście Komisji powinno uwzględniać inicjatywy polityczne UE oraz przepisy dotyczące bezpieczeństwa sieci i informacji, normy branżowe i dobre praktyki, aby było zgodne ze wszystkimi odpowiednimi przepisami i umożliwiało interoperacyjność i kompatybilność.

(8) Departamenty Komisji odpowiedzialne za systemy teleinformatyczne powinny opracować i wdrożyć odpowiednie środki, a środki bezpieczeństwa informatycznego mające na celu ochronę systemów teleinformatycznych powinny być koordynowane w całej Komisji, by zapewnić ich wydajność i skuteczność.

(9) Przepisy i procedury w zakresie dostępu do informacji w kontekście bezpieczeństwa IT, w tym reagowania na incydenty związane z bezpieczeństwem informacji, powinny być proporcjonalne do zagrożenia dla Komisji lub jej personelu i zgodne z zasadami ustanowionymi w rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([1]) o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy unijne i o swobodnym przepływie takich danych, a także uwzględniać kwestie tajemnicy zawodowej, jak przewidziano w art. 339 TFUE.

([1]) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

(10) Polityka i przepisy dotyczące systemów teleinformatycznych przetwarzających informacje niejawne UE (EUCI), szczególnie chronione informacje jawne i informacje jawne muszą być w pełni zgodne z decyzjami Komisji (UE, Euratom) 2015/443 ([1]) i (UE, Euratom) 2015/444 ([2]).

(11) Komisja powinna dokonać przeglądu swoich przepisów dotyczących bezpieczeństwa systemów teleinformatycznych wykorzystywanych przez Komisję oraz uaktualnić te przepisy.

(12) Należy zatem uchylić decyzję Komisji C(2006) 3602,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsza decyzja ma zastosowanie do wszystkich systemów teleinformatycznych (CIS) posiadanych, zamawianych, zarządzanych i obsługiwanych przez Komisję lub w jej imieniu oraz do każdorazowego wykorzystania przedmiotowych CIS przez Komisję.

2. W niniejszej decyzji ustanawia się podstawowe zasady, cele, organizację i obowiązki dotyczące bezpieczeństwa wspomnianych CIS, w szczególności w odniesieniu do departamentów Komisji posiadających, zamawiających, zarządzających lub obsługujących CIS, w tym CIS zapewnianych przez wewnętrznego dostawcę usług informatycznych. Jeżeli CIS jest zapewniany, posiadany, zarządzany lub obsługiwany przez podmiot zewnętrzny na podstawie porozumienia dwustronnego lub umowy dwustronnej z Komisją, postanowienia tego rodzaju porozumienia lub umowy muszą być zgodne z niniejszą decyzją.

3. Niniejsza decyzja ma zastosowanie do wszystkich departamentów Komisji i agencji wykonawczych. Jeżeli z CIS Komisji korzystają inne organy i instytucje na podstawie porozumienia dwustronnego z Komisją, postanowienia tego porozumienia muszą być zgodne z niniejszą decyzją.

4. Bez uszczerbku dla jakichkolwiek konkretnych wskazań dotyczących poszczególnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Komisji, pracowników Komisji objętych regulaminem pracowniczym urzędników Unii Europejskiej („regulamin pracowniczy") i warunkami zatrudnienia innych pracowników Unii Europejskiej ([3]), ekspertów krajowych oddelegowanych do Komisji („oddelegowani eksperci krajowi") ([4]), zewnętrznych dostawców usług i ich pracowników, stażystów oraz do wszystkich osób mających dostęp do CIS objętego zakresem niniejszej decyzji.

5. Niniejsza decyzja ma zastosowanie do Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) w zakresie, w jakim jest zgodna z przepisami Unii i z decyzją Komisji 1999/352/WE, EWWiS, Euratom ([5]). W szczególności środków przewidzianych w niniejszej decyzji, w tym instrukcji, inspekcji, dochodzeń i środków równoważnych, nie można stosować w odniesieniu do CIS Urzędu, jeżeli narusza to niezależność funkcji dochodzeniowej Urzędu lub poufność informacji otrzymanych przez Urząd w ramach sprawowanej przez niego funkcji.

Artykuł 2

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

1) „rozliczany" oznacza odpowiadający za działania, decyzje i wyniki;

([1]) Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41).
([2]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).
([3]) Ustanowione rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiającego regulamin pracowniczy urzędników Wspólnot Europejskich i warunki zatrudnienia innych pracowników Wspólnot oraz ustanawiającego specjalne środki stosowane tymczasowo wobec urzędników Komisji (warunki zatrudnienia innych pracowników) (Dz.U. L 56 z 4.3.1968, s. 1).
([4]) Decyzja Komisji z dnia 12 listopada 2008 r. dotycząca zasad mających zastosowanie do oddelegowanych ekspertów krajowych i ekspertów krajowych odbywających kształcenie zawodowe w ramach służb Komisji (C(2008) 6866 final).
([5]) Decyzja Komisji 1999/352/ WE, EWWiS, Euratom z dnia 28 kwietnia 1999 r. ustanawiająca Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) (Dz.U. L 136 z 31.5.1999, s. 20).

2) „CERT–UE" oznacza zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE. Jego zadaniem jest wspieranie instytucji europejskich w zakresie ochrony przed umyślnymi i złośliwymi atakami, które mogłyby naruszyć integralność ich aktywów IT i narazić na szkodę interesy UE. Zakres działań CERT–UE obejmuje zapobieganie, wykrywanie, reagowanie i przywracanie;

3) „departament Komisji" oznacza każdą dyrekcję generalną lub służbę Komisji lub każdy gabinet członka Komisji;

4) „organ ds. bezpieczeństwa Komisji" odnosi się do roli ustanowionej w decyzji (UE, Euratom) 2015/444;

5) „system teleinformatyczny" lub „CIS" oznacza każdy system umożliwiający przetwarzanie informacji w formie elektronicznej, w tym wszystkie zasoby niezbędne do jego działania, a także infrastrukturę, organizację, pracowników i zasoby informatyczne. Definicja ta obejmuje aplikacje biznesowe, wspólne usługi IT, systemy obsługiwane na zewnątrz oraz urządzenia użytkownika końcowego;

6) „Rada Zarządzania Korporacyjnego" zapewnia najwyższy poziom nadzoru zarządzania korporacyjnego w zakresie kwestii operacyjnych i administracyjnych w Komisji;

7) „właściciel danych" oznacza osobę odpowiedzialną za zapewnienie ochrony i wykorzystania konkretnych danych przetwarzanych przez CIS;

8) „zbiór danych" oznacza zbiór informacji przeznaczony do celów konkretnego procesu biznesowego lub działania Komisji;

9) „procedura awaryjna" oznacza uprzednio określony zbiór metod i obowiązków na potrzeby reagowania na nagłe sytuacje, mających zapobiec istotnemu oddziaływaniu na Komisję;

10) „polityka w zakresie bezpieczeństwa informacji" oznacza zbiór celów związanych z bezpieczeństwem informacji, które są lub mają zostać ustanowione, wdrożone i sprawdzone. Obejmuje ona między innymi decyzje (UE, Euratom) 2015/444 i (UE, Euratom) 2015/443;

11) „Rada Sterująca ds. Bezpieczeństwa Informacji" oznacza organ zarządzający, który wspiera Radę Zarządzania Korporacyjnego w jej zadaniach związanych z bezpieczeństwem IT;

12) „wewnętrzny dostawca usług IT" oznacza departament Komisji świadczący wspólne usługi IT;

13) „bezpieczeństwo IT" lub „bezpieczeństwo CIS" oznacza zachowanie poufności, integralności i dostępności CIS oraz zbiorów danych, które są w nich przetwarzane;

14) „wytyczne w sprawie bezpieczeństwa IT" obejmują zalecane, ale dobrowolne środki, które mają na celu wsparcie norm bezpieczeństwa IT lub służą jako odniesienie w przypadku, w którym nie została wprowadzona żadna norma;

15) „incydent związany z bezpieczeństwem IT" oznacza każde zdarzenie, które mogłyby negatywnie wpłynąć na poufność, integralność lub dostępność CIS;

16) „środek bezpieczeństwa IT" oznacza środek techniczny lub organizacyjny mający na celu ograniczanie ryzyka związanego z bezpieczeństwem IT;

17) „potrzeba w zakresie bezpieczeństwa IT" oznacza dokładną i jednoznaczną definicję poziomów poufności, integralności i dostępności związanych z informacją lub systemem IT w celu określenia wymaganego poziomu ochrony;

18) „cel związany z bezpieczeństwem IT" oznacza oświadczenie o zamiarze przeciwdziałania określonym zagrożeniom lub spełnienia określonych organizacyjnych wymogów lub założeń związanych z bezpieczeństwem;

19) „plan bezpieczeństwa IT" oznacza dokumentację środków bezpieczeństwa IT, które są wymagane, by spełnić potrzeby CIS w zakresie bezpieczeństwa IT;

20) „polityka w zakresie bezpieczeństwa IT" oznacza zbiór celów związanych z bezpieczeństwem IT, które są lub mają zostać ustanowione, wdrożone i sprawdzone. Obejmuje ona niniejszą decyzję i jej przepisy wykonawcze;

21) „wymóg bezpieczeństwa IT" oznacza potrzebę w zakresie bezpieczeństwa IT sformalizowaną za pośrednictwem uprzednio zdefiniowanego procesu;

22) „ryzyko związane z bezpieczeństwem IT" oznacza wpływ, jaki zagrożenie dla bezpieczeństwa IT może wywrzeć na CIS, wykorzystując jego podatność; ryzyko związane z bezpieczeństwem IT jako takie charakteryzują dwa czynniki: 1) niepewność, tj. prawdopodobieństwo, że zagrożenie związane z bezpieczeństwem IT spowoduje niepożądane zdarzenie; oraz 2) wpływ, tj. konsekwencje, jakie tego rodzaju niepożądane zdarzenie może mieć dla CIS;

23) „normy bezpieczeństwa IT" oznaczają szczególne obowiązkowe środki bezpieczeństwa IT, które ułatwiają egzekwowanie i wspieranie polityki w zakresie bezpieczeństwa IT;

24) „strategia bezpieczeństwa IT" oznacza zbiór projektów i działań, które mają ułatwić realizację celów Komisji i które muszą zostać ustanowione, wdrożone i sprawdzone;

25) „zagrożenie związane z bezpieczeństwem IT" oznacza czynnik mogący potencjalnie doprowadzić do niepożądanego zdarzenia, które może zaszkodzić CIS; tego rodzaju zagrożenia mogą być przypadkowe lub zamierzone i obejmują elementy zagrażające, potencjalne cele i metody ataku;

26) „lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego" oznacza urzędnika odpowiedzialnego za kontakty w zakresie bezpieczeństwa IT w danym departamencie Komisji;

27) „dane osobowe", „przetwarzanie danych osobowych", „administrator danych" i „zbiór danych osobowych" mają takie samo znaczenie jak w rozporządzeniu (WE) nr 45/2001, w szczególności w jego art. 2;

28) „przetwarzanie informacji" oznacza wszystkie funkcje CIS w odniesieniu do zbiorów danych, w tym tworzenie, modyfikację, wyświetlanie, przechowywanie, przesyłanie, usuwanie i archiwizowanie informacji; CIS może zapewniać przetwarzanie informacji jako zbiór funkcji na potrzeby użytkowników i jako usługi IT w stosunku do innych CIS;

29) „tajemnica zawodowa" oznacza ochronę informacji związanych z danymi biznesowymi objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych zgodnie z art. 339 TFUE;

30) „odpowiedzialny" oznacza zobowiązany do działania i podejmowania decyzji w celu osiągnięcia wymaganych wyników;

31) „bezpieczeństwo w Komisji" oznacza bezpieczeństwo osób, mienia i informacji w Komisji, a w szczególności integralność fizyczną osób i mienia, integralność, poufność i dostępność informacji i systemów teleinformatycznych, jak również swobodne funkcjonowanie działań Komisji;

32) „wspólna usługa IT" oznacza usługę świadczoną przez CIS na rzecz innych CIS w zakresie przetwarzania informacji;

33) „właściciel systemu" oznacza jednostkę odpowiedzialną w ogólnym ujęciu za udzielenie zamówienia na CIS, jego opracowywanie, integrację, modyfikację, działanie, utrzymywanie i wycofanie;

34) „użytkownik" oznacza każdą osobę wykorzystującą funkcję zapewnianą przez CIS zarówno w samej Komisji, jak i poza nią.

Artykuł 3

Zasady bezpieczeństwa IT w Komisji

1. Bezpieczeństwo IT w Komisji opiera się na zasadach legalności, przejrzystości, proporcjonalności i odpowiedzialności.

2. Kwestie związane z bezpieczeństwem IT uwzględnia się od początku procesu opracowywania i wdrażania CIS Komisji. W tym celu zaangażowane są Dyrekcja Generalna ds. Informatyki i Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa w ramach ich odpowiednich zakresów odpowiedzialności.

3. Skuteczne bezpieczeństwo IT zapewnia odpowiednie poziomy:

a) autentyczności: gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł;

b) dostępności: cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu;

c) poufności: cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom lub podmiotom ani do celów nieuprawnionego przetwarzania;

d) integralności: cecha polegająca na zachowywaniu dokładności i kompletności zasobów i informacji;

e) niezaprzeczalności: możliwość udowodnienia, że działanie lub zdarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub zdarzenia.

f) ochrony danych osobowych: zapewnianie odpowiednich zabezpieczeń w odniesieniu do danych osobowych jest w pełni zgodne z rozporządzeniem (WE) nr 45/2001;

g) tajemnicy zawodowej: ochrona informacji objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych zgodnie z art. 339 TFUE.

4. Bezpieczeństwo IT opiera się na procesie zarządzania ryzykiem. Celem tego procesu jest określenie poziomów rodzajów ryzyka związanego z bezpieczeństwem IT i określenie środków bezpieczeństwa mających na celu ograniczenie takich rodzajów ryzyka do określonego poziomu przy zachowaniu proporcjonalnych kosztów.

5. Każdy CIS musi zostać zidentyfikowany, przypisany do właściciela systemu i zapisany w wykazie.

6. Wymogi dotyczące bezpieczeństwa wszystkich CIS określa się na podstawie ich potrzeb w zakresie bezpieczeństwa oraz potrzeb w zakresie bezpieczeństwa informacji, które przetwarzają. CIS, które świadczą usługi na rzecz innych CIS, mogą być projektowane w taki sposób, aby wspierać określone poziomy potrzeb w zakresie bezpieczeństwa.

7. Plany bezpieczeństwa IT i środki bezpieczeństwa IT są proporcjonalne do potrzeb w zakresie bezpieczeństwa CIS.

Procesy związane z tymi zasadami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

ROZDZIAŁ 2

ORGANIZACJA I ZAKRES OBOWIĄZKÓW

Artykuł 4

Rada Zarządzania Korporacyjnego

Rada Zarządzania Korporacyjnego ponosi ogólną odpowiedzialność za zarządzanie całym bezpieczeństwem IT w Komisji.

Artykuł 5

Rada Sterująca ds. Bezpieczeństwa Informacji

1. Radzie Sterującej ds. Bezpieczeństwa Informacji przewodniczy Zastępca Sekretarza Generalnego odpowiedzialny za zarządzaniem bezpieczeństwem IT w Komisji. Jej członkowie reprezentują interesy związane z biznesem, technologią i bezpieczeństwem w departamentach Komisji oraz obejmują przedstawicieli Dyrekcji Generalnej ds. Informatyki, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, Dyrekcji Generalnej ds. Budżetu oraz zmieniających się co dwa lata na zasadzie rotacji przedstawicieli czterech innych zaangażowanych departamentów Komisji, w których bezpieczeństwo IT stanowi ważny aspekt w kontekście ich działań. Członkami są osoby należące do kadry kierowniczej wyższego szczebla.

2. Rada Sterująca ds. Bezpieczeństwa Informacji wspiera Radę Zarządzania Korporacyjnego w wykonywaniu jej zadań związanych z bezpieczeństwem IT. Rada Sterująca ds. Bezpieczeństwa Informacji ponosi odpowiedzialność operacyjną za zarządzanie całością bezpieczeństwa IT w Komisji.

3. Rada Sterująca ds. Bezpieczeństwa Informacji zaleca politykę Komisji w zakresie bezpieczeństwa IT, którą Komisja powinna przyjąć.

4. Dwa razy w roku Rada Sterująca ds. Bezpieczeństwa Informacji dokonuje przeglądu kwestii związanych z zarządzaniem, jak również kwestii związanych z bezpieczeństwem IT, w tym poważnych incydentów związanych z bezpieczeństwem IT, i składa sprawozdania na ten temat Radzie Zarządzania.

5. Rada Sterująca ds. Bezpieczeństwa Informacji monitoruje ogólne wdrożenie niniejszej decyzji oraz przeprowadza jego przegląd i składa Radzie Zarządzania Korporacyjnego sprawozdania na ten temat.

6. Na wniosek Dyrekcji Generalnej ds. Informatyki Rada Sterująca ds. Bezpieczeństwa Informacji dokonuje przeglądu wdrożenia aktualnej strategii bezpieczeństwa IT oraz zatwierdza i monitoruje jej wdrażanie. Rada Sterująca ds. Bezpieczeństwa Informacji składa Radzie Zarządzania Korporacyjnego sprawozdania na ten temat.

7. Rada Sterująca ds. Bezpieczeństwa Informacji monitoruje, ocenia i kontroluje sytuację w zakresie postępowania z ryzykiem, na które narażone są informacje korporacyjne, oraz posiada uprawnienie do wydawania w stosownych przypadkach formalnych wymogów w zakresie poprawy sytuacji.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 6

Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa

W odniesieniu do bezpieczeństwa IT na Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa ciążą poniższe obowiązki. Dyrekcja ta:

1) zapewnia dostosowanie polityki w zakresie bezpieczeństwa IT i polityki Komisji w zakresie bezpieczeństwa informacji;

2) ustanawia ramy na potrzeby upoważnienia do stosowania technologii szyfrujących w zakresie przechowywania i przekazywania informacji za pośrednictwem CIS;

3) informuje Dyrekcję Generalną ds. Informatyki o konkretnych zagrożeniach, które mogą mieć istotny wpływ na bezpieczeństwo CIS i zbiorów danych, które są w nich przetwarzane;

4) przeprowadza kontrole bezpieczeństwa IT, aby ocenić zgodność CIS Komisji z polityką w zakresie bezpieczeństwa, oraz przedstawia ich wyniki Radzie Sterującej ds. Bezpieczeństwa Informacji;

5) ustanawia ramy w zakresie upoważnienia dostępu do CIS Komisji z sieci zewnętrznych oraz powiązanych odpowiednich przepisów bezpieczeństwa, a także opracowuje odpowiednie normy bezpieczeństwa IT i wytyczne w sprawie bezpieczeństwa IT w ścisłej współpracy z Dyrekcją Generalną ds. Informatyki;

6) proponuje zasady i przepisy dotyczące outsourcingu CIS, aby utrzymać właściwą kontrolę bezpieczeństwa informacji;

7) opracowuje odpowiednie normy bezpieczeństwa IT oraz wytyczne w sprawie bezpieczeństwa IT w związku z art. 6, w ścisłej współpracy z Dyrekcją Generalną ds. Informatyki.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 7

Dyrekcja Generalna ds. Informatyki

W odniesieniu do ogólnego bezpieczeństwa IT Komisji na Dyrekcji Generalnej ds. Informatyki ciążą poniższe obowiązki. Dyrekcja ta:

1) opracowuje normy bezpieczeństwa IT oraz wytyczne w sprawie bezpieczeństwa IT, z wyjątkiem przewidzianych w art. 6, w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu zapewnienia spójności między polityką w zakresie bezpieczeństwa IT a polityką Komisji w zakresie bezpieczeństwa informacji oraz przedstawia je Radzie Sterującej ds. Bezpieczeństwa Informacji;

2) ocenia metody, procesy i wyniki zarządzania rodzajami ryzyka związanego z bezpieczeństwem IT w odniesieniu do wszystkich departamentów Komisji i składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

3) przedstawia bieżącą strategię bezpieczeństwa IT Radzie Sterującej ds. Bezpieczeństwa Informacji do przeglądu i zatwierdzenia, a następnie przyjęcia przez Radę Zarządzania Korporacyjnego, oraz przedstawia program, w tym planowanie projektów i działań mających na celu wdrożenie strategii bezpieczeństwa IT;

4) monitoruje realizację strategii bezpieczeństwa IT Komisji i składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

5) monitoruje rodzaje ryzyka związanego z bezpieczeństwem IT i środki bezpieczeństwa IT wdrożone w CIS oraz składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

6) składa regularnie Radzie Sterującej ds. Bezpieczeństwa Informacji sprawozdania na temat ogólnego wykonania i przestrzegania niniejszej decyzji;

7) po konsultacjach z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa wymaga od właścicieli systemów podjęcia określonych środków bezpieczeństwa IT w celu ograniczenia rodzajów ryzyka związanego z bezpieczeństwem IT, na jakie narażone są CIS Komisji;

8) zapewnia, aby właściciele systemów i właściciele danych mieli dostęp do odpowiedniego katalogu usług w zakresie bezpieczeństwa IT Dyrekcji Generalnej ds. Informatyki, dzięki któremu będą mogli wywiązać się ze swoich obowiązków związanych z bezpieczeństwem IT oraz stosować się do polityki w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT;

9) zapewnia właścicielom systemu i właścicielom danych odpowiednią dokumentację oraz konsultuje się z nimi, w stosownych przypadkach, w sprawie środków bezpieczeństwa IT wdrażanych na potrzeby ich usług IT w celu ułatwienia im zachowania zgodności z polityką w zakresie bezpieczeństwa IT oraz wspierania właścicieli systemów w zarządzaniu ryzykiem w obszarze IT;

10) organizuje regularne spotkania sieci lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego (LISO) i wspiera ich w wykonywaniu ich obowiązków;

11) określa potrzeby szkoleniowe i koordynuje programy szkoleniowe w zakresie bezpieczeństwa IT we współpracy z departamentami Komisji oraz opracowuje, wdraża i koordynuje kampanie na rzecz poszerzania wiedzy w obszarze bezpieczeństwa IT w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

12) zapewnia, aby właściciele systemów, właściciele danych oraz inne podmioty pełniące funkcje związane z bezpieczeństwem IT w departamentach Komisji zapoznali się z polityką w zakresie bezpieczeństwa IT;

13) powiadamia Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa o określonych zagrożeniach związanych z bezpieczeństwem IT, incydentach i wyjątkach dotyczących polityki Komisji w zakresie bezpieczeństwa IT zgłoszonych przez właścicieli systemów, które mogły znacząco wpłynąć na bezpieczeństwo w Komisji;

14) w związku ze swoją rolą wewnętrznego dostawcy usług IT przekazuje Komisji katalog wspólnych usług IT, które zapewniają określone poziomy bezpieczeństwa. Odbywa się to poprzez systematyczne ocenianie rodzajów ryzyka związanego z bezpieczeństwem IT, zarządzanie nim i monitorowanie w celu wdrożenia środków bezpieczeństwa dla osiągnięcia określonego poziomu bezpieczeństwa.

Powiązane procesy i bardziej szczegółowe obowiązki zostają doprecyzowane w przepisach wykonawczych.

Artykuł 8

Departamenty Komisji

W odniesieniu do bezpieczeństwa IT w swoim departamencie każdy szef departamentu Komisji:

1) w odniesieniu do każdego CIS – formalnie wyznacza właściciela systemu, będącego urzędnikiem lub pracownikiem zatrudnionym na czas określony, który będzie odpowiadał za bezpieczeństwo IT tego systemu, a także w odniesieniu do każdego zbioru danych przechowywanego w CIS – formalnie wyznacza właściciela danych, który powinien należeć do tej samej jednostki administracyjnej będącej administratorem danych w odniesieniu do zbiorów danych podlegających rozporządzeniu (WE) nr 45/2001;

2) formalnie wyznacza lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego, który może pełnić obowiązki niezależnie od właścicieli systemów i właścicieli danych. Lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego można przypisać do jednego lub kilku departamentów Komisji;

3) zapewnia, aby opracowane i wdrożone zostały odpowiednie oceny rodzajów ryzyka związanego z bezpieczeństwem IT oraz plany bezpieczeństwa IT;

4) zapewnia regularne przekazywanie Dyrekcji Generalnej ds. Informatyki podsumowania rodzajów ryzyka i środków związanych z bezpieczeństwem IT;

5) zapewnia, przy wsparciu Dyrekcji Generalnej ds. Informatyki, wprowadzanie odpowiednich procesów, procedur i rozwiązań celem zapewnienia efektywnego wykrywania, zgłaszania i rozwiązywania incydentów związanych z bezpieczeństwem IT ich systemów teleinformatycznych;

6) uruchamia procedury awaryjne w przypadku zagrożenia bezpieczeństwa IT;

7) spoczywa na nim ostateczna odpowiedzialność za bezpieczeństwo IT, co obejmuje obowiązki właściciela systemu i właściciela danych;

8) jest właściwy w odniesieniu do rodzajów ryzyka dotyczącego jego systemów teleinformatycznych i zbiorów danych;

9) rozstrzyga wszystkie spory między właścicielami danych a właścicielami systemów, a w przypadku utrzymywania się sporu przekazuje sprawę Radzie Sterującej ds. Bezpieczeństwa Informacji do rozstrzygnięcia;

10) zapewnia wdrożenie planów bezpieczeństwa IT i środków bezpieczeństwa IT oraz odpowiednie uwzględnienie zagrożeń.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 9

Właściciele systemów

1. Właściciel systemu jest odpowiedzialny za bezpieczeństwo IT systemu teleinformatycznego i składa sprawozdania szefowi departamentu Komisji.

2. W odniesieniu do bezpieczeństwa IT właściciel systemu:

a) zapewnia zgodność CIS z polityką w zakresie bezpieczeństwa IT;

b) zapewnia dokładne zarejestrowanie CIS w stosownym wykazie;

c) ocenia rodzaje ryzyka związanego z bezpieczeństwem IT i określa potrzeby w zakresie bezpieczeństwa IT w odniesieniu do każdego CIS, we współpracy z właścicielami danych i w porozumieniu z Dyrekcją Generalną ds. Informatyki;

d) przygotowuje plan bezpieczeństwa, w tym, w stosownych przypadkach, szczegółowe informacje na temat ocenionych rodzajów ryzyka oraz wszelkich dodatkowych wymaganych środków bezpieczeństwa;

e) wdraża odpowiednie środki bezpieczeństwa IT, proporcjonalne do zidentyfikowanych rodzajów ryzyka związanego z bezpieczeństwem IT, i postępuje zgodnie z zaleceniami zatwierdzonymi przez Radę Sterującą ds. Bezpieczeństwa Informacji;

f) określa wszelkie zależności od innych systemów teleinformatycznych lub wspólnych usług IT oraz, w stosownych przypadkach, wdraża środki bezpieczeństwa na podstawie poziomów bezpieczeństwa zaproponowanych przez te systemy teleinformatyczne lub wspólne usługi IT;

g) zarządza rodzajami ryzyka związanego z bezpieczeństwem IT i je monitoruje;

h) regularnie zgłasza szefowi departamentu Komisji profil ryzyka związanego z bezpieczeństwem IT swojego CIS oraz powiadamia Dyrekcję Generalną ds. Informatyki o powiązanych rodzajach ryzyka, działaniach z zakresu zarządzania ryzykiem oraz podjętych środkach bezpieczeństwa;

i) konsultuje z lokalnym pełnomocnikiem ds. bezpieczeństwa teleinformatycznego z odpowiedniego departamentu Komisji kwestie związane z bezpieczeństwem IT;

j) wydaje instrukcje dla użytkowników dotyczące korzystania z CIS i powiązanych danych oraz dotyczące obowiązków użytkowników związanych z CIS;

k) działając jako organ ds. kryptograficznych, wymaga od Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa upoważnienia w odniesieniu do każdego CIS korzystającego z technologii szyfrowania;

l) z wyprzedzeniem konsultuje się z organem ds. bezpieczeństwa Komisji w sprawie każdego systemu przetwarzania informacji niejawnych UE;

m) zapewnia przechowywanie kopii zapasowych wszystkich kluczy deszyfrujących w depozycie. Odzyskiwanie zaszyfrowanych danych przeprowadza się tylko wtedy, gdy jest to dozwolone zgodnie z ramami określonymi przez Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

n) przestrzega przekazanych przez odpowiedniego administratora danych instrukcji, które dotyczą ochrony danych osobowych oraz stosowania przepisów o ochronie danych na temat bezpieczeństwa przetwarzania danych;

o) powiadamia Dyrekcję Generalną ds. Informatyki o wszelkich odstępstwach od polityki Komisji w zakresie bezpieczeństwa IT, w tym o odpowiednich uzasadnieniach;

p) zgłasza szefowi departamentu Komisji wszelkie nierozwiązywalne spory między właścicielem danych a właścicielem systemu oraz, stosownie do przypadku, powiadamia w odpowiednim czasie odpowiednie zainteresowane strony o incydentach związanych z bezpieczeństwem IT w zależności od ich stopnia zagrożenia zgodnie z art. 15;

q) w odniesieniu do systemów zewnętrznych zapewnia uwzględnienie odpowiednich przepisów dotyczących bezpieczeństwa IT w umowach outsourcingowych oraz zgłoszenie incydentów związanych z bezpieczeństwem IT występujących w zewnętrznym CIS zgodnie z art. 15;

r) w odniesieniu do CIS zapewniającego wspólne usługi IT zapewnia i jasno dokumentuje określony poziom bezpieczeństwa oraz zapewnia wdrożenie środków bezpieczeństwa w odniesieniu do tego CIS w celu osiągnięcia określonego poziomu bezpieczeństwa.

3. Właściciele systemów mogą formalnie przekazywać część lub całość swoich zadań związanych z bezpieczeństwem IT, nadal jednak pozostają odpowiedzialni za bezpieczeństwo IT swojego CIS.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 10

Właściciele danych

1. Właściciel danych jest odpowiedzialny za bezpieczeństwo IT określonego zbioru danych przed szefem departamentu Komisji oraz jest rozliczany z kwestii poufności, integralności i dostępności zbioru danych.

2. W odniesieniu do tego zbioru danych właściciel danych:

a) zapewnia właściwą klasyfikację wszystkich zbiorów danych, za które odpowiada, zgodnie z decyzjami (UE, Euratom) 2015/443 i (UE, Euratom) 2015/444;

b) określa potrzeby w zakresie bezpieczeństwa informacji i informuje odpowiednich właścicieli systemów o tych potrzebach;

c) uczestniczy w ocenie ryzyka dotyczącej CIS;

d) zgłasza szefowi departamentu Komisji wszelkie nierozwiązywalne spory między właścicielem danych a właścicielem systemu;

e) zgłasza incydenty związane z bezpieczeństwem IT, jak przewidziano w art. 15.

3. Właściciele danych mogą formalnie przekazywać część lub całość swoich zadań związanych z bezpieczeństwem IT, nadal jednak zachowują zakres odpowiedzialności określony w niniejszym artykule.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 11

Lokalni pełnomocnicy ds. bezpieczeństwa teleinformatycznego

W odniesieniu do bezpieczeństwa IT lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego:

a) aktywnie identyfikuje właścicieli systemów, właścicieli danych i inne podmioty pełniące funkcje związane z bezpieczeństwem IT w departamentach Komisji oraz informuje ich o polityce w zakresie bezpieczeństwa IT;

b) w ramach sieci lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego kontaktuje się z Dyrekcją Generalną ds. Informatyki w sprawach dotyczących bezpieczeństwa IT w departamentach Komisji;

c) uczestniczy w organizowanych regularnie spotkaniach lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego;

d) prowadzi przegląd procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji oraz przegląd procesu opracowywania i wdrażania planów bezpieczeństwa w odniesieniu do systemów informatycznych;

e) doradza właścicielom danych, właścicielom systemów i szefom departamentów Komisji w kwestiach związanych z bezpieczeństwem IT;

f) wspólnie z Dyrekcją Generalną ds. Informatyki rozpowszechnia dobre praktyki w zakresie bezpieczeństwa IT oraz proponuje określone programy uświadamiające i szkoleniowe;

g) przedkłada szefowi departamentu Komisji sprawozdania dotyczące bezpieczeństwa IT oraz określa braki i usprawnienia.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 12

Użytkownicy

1. W odniesieniu do bezpieczeństwa IT użytkownicy:

a) postępują zgodnie z polityką w zakresie bezpieczeństwa IT i wydanymi przez właściciela systemu instrukcjami dotyczącymi korzystania z danego CIS;

b) zgłaszają incydenty związane z bezpieczeństwem IT, jak przewidziano w art. 15.

2. Korzystanie z CIS Komisji z naruszeniem polityki w zakresie bezpieczeństwa IT lub instrukcji wydanych przez właściciela systemu może stanowić podstawę do wszczęcia postępowania dyscyplinarnego.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

ROZDZIAŁ 3

WYMOGI I OBOWIĄZKI ZWIĄZANE Z BEZPIECZEŃSTWEM

Artykuł 13

Wykonanie niniejszej decyzji

1. Przyjęcie przepisów wykonawczych dotyczących art. 6, a także związanych z nimi norm i wytycznych, będzie przedmiotem decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa.

2. Przyjęcie wszystkich pozostałych przepisów wykonawczych do niniejszej decyzji, a także związanych z nimi norm bezpieczeństwa IT i wytycznych w sprawie bezpieczeństwa IT, będzie przedmiotem decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie informatyczne.

3. Rada Sterująca ds. Bezpieczeństwa Informacji zatwierdza przepisy wykonawcze, normy i wytyczne wspomniane w ust. 1 i 2 powyżej przed ich przyjęciem.

Artykuł 14

Obowiązek przestrzegania

1. Przestrzeganie przepisów opisanych w polityce w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT jest obowiązkowe.

2. Nieprzestrzeganie polityki w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT może pociągać za sobą odpowiedzialność dyscyplinarną zgodnie z traktatami, regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Wspólnot Europejskich oraz sankcje umowne lub czynności prawne wynikające z krajowych przepisów ustawowych i wykonawczych.

3. Dyrekcję Generalną ds. Informatyki powiadamia się o wszelkich odstępstwach od polityki w zakresie bezpieczeństwa IT.

4. Jeżeli Rada Sterująca ds. Bezpieczeństwa Informacji stwierdza, że istnieje stałe niedopuszczalne ryzyko związane z CIS Komisji, Dyrekcja Generalna ds. Informatyki we współpracy z właścicielem systemu proponuje środki ograniczające ryzyko, które podlegają zatwierdzeniu przez Radę Sterującą ds. Bezpieczeństwa Informacji. Środki te mogą, między innymi, obejmować wzmocnione monitorowanie i sprawozdawczość, ograniczenia usług i odłączenie.

5. W razie potrzeby Rada Sterująca ds. Bezpieczeństwa Informacji nakłada obowiązek wdrożenia zatwierdzonych środków ograniczających ryzyko. Rada Sterująca ds. Bezpieczeństwa Informacji może również zalecić Dyrektorowi Generalnemu Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa wszczęcie postępowania administracyjnego. Dyrekcja Generalna ds. Informatyki informuje Radę Sterującą ds. Bezpieczeństwa Informacji o każdej sytuacji, w której zastosowano środki ograniczające ryzyko.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

Artykuł 15

Reagowanie na incydenty związane z bezpieczeństwem IT

1. Dyrekcja Generalna ds. Informatyki jest odpowiedzialna za zapewnienie głównej operacyjnej zdolności reagowania na incydenty związane z bezpieczeństwem IT w Komisji Europejskiej.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, jako zainteresowana strona mająca swój udział w reagowaniu na incydenty związane z bezpieczeństwem IT:

a) ma prawo dostępu do informacji zbiorczych zawartych we wszystkich rejestrach incydentów i pełnych rejestrów po złożeniu stosownego wniosku;

b) uczestniczy w działaniach grup ds. zarządzania sytuacjami kryzysowymi obejmującymi incydenty związane z bezpieczeństwem IT oraz w procedurach awaryjnych związanych z bezpieczeństwem IT;

c) odpowiada za kontakty z organami ścigania i służbami wywiadowczymi;

d) wykonuje analizę kryminalistyczną dotyczącą bezpieczeństwa cybernetycznego zgodnie z art. 11 decyzji (UE, Euratom) 2015/443;

e) podejmuje decyzje w sprawie wszczęcia formalnego postępowania;

f) powiadamia Dyrekcję Generalną ds. Informatyki o wszelkich incydentach związanych z bezpieczeństwem IT, które mogą zagrażać innym CIS.

3. Dyrekcja Generalna ds. Informatyki regularnie komunikuje się z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu wymiany informacji i koordynowania reakcji na incydenty związane z bezpieczeństwem IT, które mogą wymagać wszczęcia formalnego postępowania.

4. W stosownych przypadkach usługi w zakresie koordynowania reakcji na incydenty – oferowane instytucjom, organom i agencjom UE przez zespół reagowania na incydenty komputerowe („CERT–UE") – mogą być wykorzystywane do wspierania procesu reagowania na incydenty oraz wymiany wiedzy z innymi zagrożonymi instytucjami i agencjami UE.

5. Właściciele systemów uczestniczący w incydencie związanym z bezpieczeństwem IT:

a) niezwłocznie powiadamiają swoich szefów departamentów Komisji, Dyrekcję Generalną ds. Informatyki, Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa, lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego oraz, w stosownych przypadkach, właściciela danych o wszelkich poważnych incydentach związanych z bezpieczeństwem IT, w szczególności tych, które dotyczą naruszenia poufności danych;

b) współpracują z odpowiednimi organami Komisji i przestrzegają ich instrukcji dotyczących zgłaszania incydentów, reagowania na nie i stosowania środków zaradczych.

6. Użytkownicy powiadamiają w stosownym czasie odpowiedni helpdesk IT o wszystkich rzeczywistych lub podejrzewanych incydentach związanych z bezpieczeństwem IT.

7. Właściciele danych powiadamiają w stosownym czasie zespół reagowania na incydenty związane z bezpieczeństwem IT o wszystkich rzeczywistych lub podejrzewanych incydentach związanych z bezpieczeństwem IT.

8. Dyrekcja Generalna ds. Informatyki, przy wsparciu innych uczestniczących zainteresowanych stron, jest odpowiedzialna za reagowanie na wszelkie incydenty związane z bezpieczeństwem IT wykryte w odniesieniu do CIS Komisji, które nie są systemami obsługiwanymi przez firmy zewnętrzne.

9. Dyrekcja Generalna ds. Informatyki powiadamia o incydentach związanych z bezpieczeństwem IT zagrożone departamenty Komisji, odpowiednich lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego oraz, w stosownych przypadkach, CERT–UE na zasadzie wiedzy koniecznej.

10. Dyrekcja Generalna ds. Informatyki składa regularnie Radzie Sterującej ds. Bezpieczeństwa Informacji sprawozdania na temat poważnych incydentów związanych z bezpieczeństwem IT, które zagrażają CIS Komisji.

11. Odpowiedni lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego uzyskuje, na wniosek, dostęp do rejestrów incydentów związanych z bezpieczeństwem IT dotyczących CIS departamentu Komisji.

12. W przypadku poważnego incydentu związanego z bezpieczeństwem IT Dyrekcja Generalna ds. Informatyki pełni rolę punktu kontaktowego na potrzeby zarządzania sytuacjami kryzysowymi poprzez koordynowanie działań grup ds. zarządzania kryzysowego na wypadek incydentów związanych z bezpieczeństwem IT.

13. W przypadku sytuacji wyjątkowej Dyrektor Generalny Dyrekcji Generalnej ds. Informatyki może zdecydować o wszczęciu procedury awaryjnej dotyczącej bezpieczeństwa IT. Dyrekcja Generalna ds. Informatyki opracowuje procedury awaryjne, które mają zostać zatwierdzone przez Radę Sterującą ds. Bezpieczeństwa Informacji.

14. Dyrekcja Generalna ds. Informatyki składa sprawozdania na temat wykonania procedur awaryjnych Radzie Sterującej ds. Bezpieczeństwa Informacji i szefom zagrożonych departamentów Komisji.

Procesy związane z tymi obowiązkami i działaniami zostają szczegółowo opisane w przepisach wykonawczych.

ROZDZIAŁ 4

PRZEPISY KOŃCOWE

Artykuł 16

Przejrzystość

Niniejsza decyzja zostaje podana do wiadomości służb Komisji i wszystkich osób, których dotyczy, oraz zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 17

Odniesienia do innych aktów

Przepisy niniejszej decyzji pozostają bez uszczerbku dla decyzji (UE, Euratom) 2015/443, decyzji (UE, Euratom) 2015/444, rozporządzenia (WE) nr 45/2001, rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([1]), decyzji 2002/47/ WE, EWWiS, Euratom ([2]), rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([3]) oraz decyzji 1999/352/WE, EWWiS, Euratom.

Artykuł 18

Uchylenie i środki przejściowe

Decyzja C(2006) 3602 z dnia 16 sierpnia 2006 r. traci moc.

Przepisy wykonawcze i normy bezpieczeństwa IT przyjęte zgodnie z art. 10 decyzji C(2006) 3602 pozostają w mocy, o ile nie są sprzeczne z niniejszą decyzją, do czasu zastąpienia ich przepisami wykonawczymi i normami, które zostaną przyjęte zgodnie z art. 13 niniejszej decyzji. Każde odniesienie do art. 10 decyzji C(2006) 3602 należy rozumieć jako odniesienie do art. 13 niniejszej decyzji.

Artykuł 19

Wejście w życie

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 10 stycznia 2017 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

([1]) Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).
([2]) Decyzja Komisji 2002/47/WE, EWWiS, Euratom z dnia 23 stycznia 2002 r. zmieniająca jej regulamin (Dz.U. L 21 z 24.1.2002, s. 23).
([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

ISSN 1977-0766 (wydanie elektroniczne)
ISSN 1725-5139 (wydanie papierowe)

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL