Dziennik Urzędowy L 72

Unii Europejskiej

Wydanie polskie

Legislacja

Tom 58

17 marca 2015

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)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/434

z dnia 16 marca 2015 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.

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

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 16 marca 2015 r.

W imieniu Komisji,

za Przewodniczącego,

Jerzy PLEWA

Dyrektor Generalny ds. Rolnictwa i Rozwoju Obszarów Wiejskich

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	EG	65,8
	MA	84,9
	TR	86,4
	ZZ	79,0
0707 00 05	JO	229,9
	MA	183,9
	TR	185,1
	ZZ	199,6
0709 93 10	MA	119,5
	TR	192,4
	ZZ	156,0
0805 10 20	EG	45,8
	IL	72,7
	MA	56,7
	TN	57,3
	TR	63,6
	ZZ	59,2
0805 50 10	TR	61,4
	ZZ	61,4
0808 10 80	BR	70,9
	CA	81,0
	CL	100,9
	CN	91,1
	MK	25,2
	US	166,1
	ZZ	89,2
0808 30 90	AR	112,0
	CL	133,2
	US	124,8
	ZA	103,5
	ZZ	118,4

(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 PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2015/435

z dnia 17 grudnia 2014 r.

w sprawie uruchomienia marginesu na nieprzewidziane wydatki

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając Porozumienie międzyinstytucjonalne z dnia 2 grudnia 2013 r. pomiędzy Parlamentem Europejskim, Radą i Komisją w sprawie dyscypliny budżetowej, współpracy w kwestiach budżetowych i należytego zarządzania finansami ([1]), w szczególności jego pkt 14,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) W art. 13 rozporządzenia Rady (UE, Euratom) nr 1311/2013 ([2]) ustanowiono na nieprzewidziane wydatki margines w wysokości do 0,03 % dochodu narodowego brutto Unii.

(2) Zgodnie z art. 6 tego rozporządzenia Komisja obliczyła bezwzględną kwotę marginesu na nieprzewidziane wydatki na rok 2014 ([3]).

(3) Po zbadaniu wszystkich innych możliwości zapewnienia środków finansowych na podejmowanie działań w nieprzewidzianych okolicznościach, które pojawiły się po tym, jak pułap płatności na 2014 r. wyznaczono po raz pierwszy w wieloletnich ramach finansowych w lutym 2013 r., uruchomienie marginesu na nieprzewidziane wydatki wydaje się konieczne w celu uzupełnienia środków na płatności w budżecie ogólnym Unii Europejskiej na rok budżetowy 2014 ponad pułap płatności.

(4) Kwotę w wysokości 350 mln EUR w środkach na płatności należy uwzględnić w ramach uruchomienia marginesu na nieprzewidziane wydatki w oczekiwaniu na porozumienie co do płatności w odniesieniu do innych instrumentów szczególnych.

(5) Biorąc pod uwagę bardzo wyjątkową sytuację, która nastąpiła w bieżącym roku, spełniony jest warunek zastosowania ostatecznego instrumentu określony w art. 13 ust. 1 rozporządzenia (UE, Euratom) nr 1311/2013.

(6) Aby zapewnić zgodność z art. 13 ust. 3 rozporządzenia (UE, Euratom) nr 1311/2013, Komisja powinna przedstawić wniosek dotyczący kompensowania stosownej kwoty pułapów płatności określonych w wieloletnich ramach finansowych na co najmniej jeden przyszły rok budżetowy, z należytym uwzględnieniem porozumienia w sprawie płatności w odniesieniu do innych instrumentów szczególnych, bez uszczerbku dla instytucjonalnych prerogatyw Komisji,

([1]) Dz.U. C 373 z 20.12.2013, s. 1.
([2]) Rozporządzenie Rady (UE, Euratom) nr 1311/2013 z dnia 2 grudnia 2013 r. określające wieloletnie ramy finansowe na lata 2014–2020 (Dz.U. L 347 z 20.12.2013, s. 884).
([3]) Komunikat Komisji do Rady i Parlamentu Europejskiego z dnia 20 grudnia 2013 r. w sprawie dostosowania technicznego ram finansowych na rok 2014 stosownie do zmian DNB (COM(2013) 928).

PRZYJMUJĄ NINIEJSZĄ DECYZJĘ:

Artykuł 1

W budżecie ogólnym Unii Europejskiej na rok budżetowy 2014 uruchamia się margines na nieprzewidziane wydatki, aby udostępnić kwotę 3 168 233 715 EUR w środkach na płatności poza i ponad pułapem płatności wieloletnich ram finansowych.

Artykuł 2

Kwota 2 818 233 715 EUR jest kompensowana w trzech ratach w marginesach wyznaczonych w ramach pułapów płatności na następujące lata:

a) 2018: 939 411 200 EUR

b) 2019: 939 411 200 EUR

c) 2020: 939 411 315 EUR.

Komisja jest proszona o przedstawienie w odpowiednim czasie wniosku dotyczącego pozostałej kwoty wynoszącej 350 mln EUR.

Artykuł 3

Niniejsza decyzja jest publikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Strasburgu dnia 17 grudnia 2014 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	B. DELLA VEDOVA
Przewodniczący	*Przewodniczący*

DECYZJA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2015/436

z dnia 17 grudnia 2014 r.

w sprawie uruchomienia Funduszu Solidarności UE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (WE) nr 2012/2002 z dnia 11 listopada 2002 r. ustanawiające Fundusz Solidarności Unii Europejskiej ([1]), w szczególności jego art. 4 ust. 3,

uwzględniając Porozumienie międzyinstytucjonalne z dnia 2 grudnia 2013 r. pomiędzy Parlamentem Europejskim, Radą i Komisją w sprawie dyscypliny budżetowej, współpracy w kwestiach budżetowych i należytego zarządzania finansami ([2]), w szczególności jego pkt 11,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Unia Europejska ustanowiła Fundusz Solidarności Unii Europejskiej („fundusz") w celu okazania solidarności z ludnością zamieszkującą regiony dotknięte klęskami.

(2) Art. 10 rozporządzenia Rady (UE, Euratom) nr 1311/2013 ([3]) pozwala uruchomić środki z funduszu w ramach rocznego pułapu wynoszącego 500 mln EUR (w cenach z 2011 r.).

(3) Rozporządzenie (WE) nr 2012/2002 zawiera przepisy umożliwiające uruchomienie funduszu.

(4) Włochy przedłożyły wniosek o uruchomienie funduszu w związku z powodziami.

(5) Grecja przedłożyła wniosek o uruchomienie funduszu w związku z trzęsieniem ziemi.

(6) Słowenia przedłożyła wniosek o uruchomienie funduszu w związku z burzami lodowymi.

(7) Chorwacja przedłożyła wniosek o uruchomienie funduszu w związku z burzami lodowymi, po których nastąpiły powodzie,

PRZYMUJĄ NINIEJSZĄ DECYZJĘ:

Artykuł 1

W ramach budżetu ogólnego Unii Europejskiej na rok budżetowy 2014 uruchamia się Fundusz Solidarności Unii Europejskiej w celu udostępnienia kwoty 46 998 528 EUR w postaci środków na zobowiązania.

W ramach budżetu ogólnego Unii Europejskiej na rok budżetowy 2015 uruchamia się Fundusz Solidarności Unii Europejskiej w celu udostępnienia kwoty 46 998 528 EUR w postaci środków na płatności.

Artykuł 2

Niniejsza decyzja zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Strasburgu dnia 17 grudnia 2014 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	B. DELLA VEDOVA
Przewodniczący	*Przewodniczący*

([1]) Dz.U. L 311 z 14.11.2002, s. 3.
([2]) Dz.U. C 373 z 20.12.2013, s. 1.
([3]) Rozporządzenie Rady (UE, Euratom) nr 1311/2013 z dnia 2 grudnia 2013 r. określające wieloletnie ramy finansowe na lata 2014–2020 (Dz.U. L 347 z 20.12.2013, s. 884).

DECYZJA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2015/437

z dnia 17 grudnia 2014 r.

w sprawie uruchomienia Funduszu Solidarności UE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (WE) nr 2012/2002 z dnia 11 listopada 2002 r. ustanawiające Fundusz Solidarności Unii Europejskiej ([1]), w szczególności jego art. 4 ust. 3,

uwzględniając Porozumienie międzyinstytucjonalne z dnia 2 grudnia 2013 r. pomiędzy Parlamentem Europejskim, Radą i Komisją w sprawie dyscypliny budżetowej, współpracy w kwestiach budżetowych i należytego zarządzania finansami ([2]), w szczególności jego pkt 11,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) Unia Europejska ustanowiła Fundusz Solidarności Unii Europejskiej („fundusz") w celu okazania solidarności z ludnością zamieszkującą regiony dotknięte klęskami.

(2) Art. 10 rozporządzenia Rady (UE, Euratom) nr 1311/2013 ([3]) pozwala uruchomić środki z funduszu w ramach rocznego pułapu wynoszącego 500 mln EUR (w cenach z 2011 r.).

(3) Rozporządzenie (WE) nr 2012/2002 zawiera przepisy, na mocy których można uruchomić fundusz.

(4) Serbia przedłożyła wniosek o uruchomienie funduszu w związku z powodziami.

(5) Chorwacja przedłożyła wniosek o uruchomienie funduszu w związku z powodziami.

(6) Bułgaria przedłożyła wniosek o uruchomienie funduszu w związku z powodziami,

PRZYJMUJĄ NINIEJSZĄ DECYZJĘ:

Artykuł 1

W ramach budżetu ogólnego Unii Europejskiej na rok budżetowy 2014 uruchamia się Fundusz Solidarności Unii Europejskiej w celu udostępnienia kwoty 79 726 440 EUR w postaci środków na zobowiązania.

W ramach budżetu ogólnego Unii Europejskiej na rok budżetowy 2015 uruchamia się Fundusz Solidarności Unii Europejskiej w celu udostępnienia kwoty 79 726 440 EUR w postaci środków na płatności.

Artykuł 2

Niniejsza decyzja jest publikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Strasburgu dnia 17 grudnia 2014 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	B. DELLA VEDOVA
Przewodniczący	*Przewodniczący*

([1]) Dz.U. L 311 z 14.11.2002, s. 3.
([2]) Dz.U. C 373 z 20.12.2013, s. 1.
([3]) Rozporządzenie Rady (UE, Euratom) nr 1311/2013 z dnia 2 grudnia 2013 r. określające wieloletnie ramy finansowe na lata 2014–2020 (Dz.U. L 347 z 20.12.2013, s. 884).

DECYZJA RADY (UE) 2015/438

z dnia 2 marca 2015 r.

określająca stanowisko, które ma zostać przyjęte w imieniu Unii Europejskiej, w ramach Wspólnego Komitetu powołanego na mocy Umowy między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz, dotyczące przyjęcia wspólnych wytycznych w sprawie wykonania tej umowy

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 77 ust. 2 lit. a) w związku z art. 218 ust. 9,

uwzględniając wniosek Komisji Europejskiej,

a także mając na uwadze, co następuje:

(1) W art. 12 Umowy między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz [1] (zwanej dalej „Umową") ustanowiono Wspólny Komitet. Artykuł ten stanowi, że Wspólny Komitet ma w szczególności kontrolować wykonanie Umowy.

(2) Umowa między Unią Europejską a Ukrainą zmieniająca Umowę między Wspólnotą Europejską a Ukrainą o ułatwieniach w wydawaniu wiz [2] (zwaną dalej „Umową zmieniającą") weszła w życie w dniu 1 lipca 2013 r.

(3) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 [3] ustanowiło procedury i warunki wydawania wiz na tranzyt przez terytorium państw członkowskich lub planowany pobyt na terytorium państw członkowskich nieprzekraczający 90 dni w ciągu każdego 180-dniowego okresu.

(4) W ramach swojego zakresu odpowiedzialności, Wspólny Komitet zwrócił uwagę na potrzebę stworzenia wspólnych wytycznych w celu zagwarantowania pełnej harmonizacji wykonywania postanowień Umowy przez konsulaty państw członkowskich oraz wyjaśnienia stosunku pomiędzy postanowieniami Umowy i przepisami umawiających się stron, które stosuje się w dalszym ciągu do kwestii wizowych nieobjętych zakresem stosowania Umowy.

(5) Wspólny Komitet przyjął takie wytyczne w dniu 25 listopada 2009 r. decyzją nr 1/2009. Przedmiotowe wytyczne powinny zostać dostosowane do nowych postanowień Umowy wprowadzonych na podstawie Umowy zmieniającej oraz do zmian w prawie wewnętrznym Unii w zakresie polityki wizowej. W celu zachowania jasności należy zastąpić te wytyczne.

(6) Należy określić stanowisko, które ma zostać przyjęte w imieniu Unii w ramach Wspólnego Komitetu, dotyczące przyjęcia wspólnych wytycznych w sprawie wykonania Umowy,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Stanowisko, które ma zostać przyjęte w imieniu Unii w ramach Wspólnego Komitetu ustanowionego na mocy art. 12 Umowy między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz, dotyczące przyjęcia wspólnych wytycznych w sprawie wykonania Umowy, opiera się na projekcie decyzji Wspólnego Komitetu dołączonym do niniejszej decyzji.

---

[1] Dz.U. L 332 z 18.12.2007, s. 68.
[2] Dz.U. L 168 z 20.6.2013, s. 11.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz.U. L 243 z 15.9.2009, s. 1).

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w Brukseli dnia 2 marca 2015 r.

W imieniu Rady
D. REIZNIECE-OZOLA
Przewodniczący

PROJEKT

DECYZJA NR …/2014 WSPÓLNEGO KOMITETU USTANOWIONEGO NA MOCY UMOWY MIĘDZY UNIĄ EUROPEJSKĄ A UKRAINĄ O UŁATWIENIACH W WYDAWANIU WIZ

z dnia …

dotycząca przyjęcia wspólnych wytycznych w sprawie jej wykonania Umowy,

WSPÓLNY KOMITET,

uwzględniając Umowę między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz (zwaną dalej „Umową"), w szczególności jej art. 12,

a także mając na uwadze, że Umowa weszła w życie dnia 1 stycznia 2008 r.,

STANOWI, CO NASTĘPUJE:

Artykuł 1

Wspólne wytyczne w sprawie wykonania Umowy między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz ustanowiono w załączniku do niniejszej decyzji.

Artykuł 2

Uchyla się decyzję Wspólnego Komitetu nr 1/2009.

Artykuł 3

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w …

W imieniu Wspólnego Komitetu *Przewodniczący*

ZAŁĄCZNIK

WSPÓLNE WYTYCZNE W CELU WYKONANIA UMOWY MIĘDZY UNIĄ EUROPEJSKĄ A UKRAINĄ O UŁATWIENIACH W WYDAWANIU WIZ

Celem Umowy między Unią Europejską a Ukrainą o ułatwieniach w wydawaniu wiz, która weszła w życie w dniu 1 stycznia 2008 r., zmienionej Umową między Unią Europejską a Ukrainą z 23 lipca 2012 r., która weszła w życie w dniu 1 lipca 2013 r. (zwanej dalej „Umową"), jest ułatwienie, na zasadzie wzajemności, procedur wydawania wiz obywatelom Ukrainy planującym pobyt nie dłuższy niż 90 dni w ciągu każdego 180-dniowego okresu.

Umowa ustanawia – na zasadzie wzajemności –wiążące prawa i obowiązki w celu uproszczenia procedur wydawania wiz dla obywateli ukraińskich.

Niniejsze wytyczne, przyjęte przez Wspólny Komitet ustanowiony na mocy art. 12 Umowy (zwany dalej „Wspólnym Komitetem"), mają na celu zapewnienie właściwego i zharmonizowanego wdrożenia postanowień Umowy przez misje dyplomatyczne i urzędy konsularne państw członkowskich. Wytyczne te nie zostały uwzględnione w Umowie i w związku z tym nie są one prawnie wiążące. Zaleca się jednak, aby pracownicy dyplomatyczni i konsularni stosowali je przy wdrażaniu postanowień Umowy.

Wytyczne należy aktualizować w świetle doświadczeń związanych z wykonaniem Umowy zgodnie z zakresem odpowiedzialności Wspólnego Komitetu. Wytyczne, przyjęte przez Wspólny Komitet w dniu 25 listopada 2009 r., zostały dostosowane, zgodnie z Umową między Unią Europejską a Ukrainą zmieniającą Umowę między Wspólnotą Europejską a Ukrainą o ułatwieniach w wydawaniu wiz (zwana dalej „Umową zmieniającą"), do nowych przepisów Unii, takich jak rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 ([1]) (zwanego dalej „kodeksem wizowym").

I. KWESTIE OGÓLNE.

1.1. **Cel oraz zakres stosowania.**

Art. 1 Umowy stanowi: „Celem niniejszej Umowy jest wprowadzenie ułatwień w wydawaniu wiz obywatelom Ukrainy planującym pobyt nie dłuższy niż 90 dni w okresie 180 dni".

Umowa ma zastosowanie do wszystkich obywateli ukraińskich ubiegających się o wizę krótkoterminową, niezależnie od państwa zamieszkania.

Art. 1 ust. 2 Umowy stanowi: „Ukraina może ponownie wprowadzić obowiązek wizowy jedynie dla obywateli lub pewnych kategorii obywateli wszystkich państw członkowskich, ale nie dla obywateli lub pewnych kategorii obywateli poszczególnych państw członkowskich. W przypadku ponownego wprowadzenia przez Ukrainę obowiązku wizowego dla obywateli UE bądź określonych grup obywateli UE, ułatwienia przewidziane w niniejszej Umowie dla obywateli ukraińskich automatycznie stają się na zasadzie wzajemności obowiązujące dla odnośnych obywateli UE".

Zgodnie z decyzjami podjętymi przez rząd Ukrainy, odpowiednio od dnia 1 maja 2005 r. lub od dnia 1 stycznia 2008 r. wszyscy obywatele UE są zwolnieni z obowiązku wizowego w przypadku podróży na Ukrainę nieprzekraczających 90 dni bądź tranzytu przez terytorium Ukrainy. Przepis ten nie narusza prawa ukraińskiego rządu do zmiany tych decyzji.

1.2. **Zakres Umowy**

Art. 2 Umowy stanowi:

„1. Ułatwienia wizowe, o których mowa w niniejszej Umowie, mają zastosowanie do obywateli Ukrainy, o ile nie są oni zwolnieni z obowiązku wizowego na mocy przepisów ustawowych i wykonawczych Unii Europejskiej lub państw członkowskich, postanowień niniejszej Umowy lub innych umów międzynarodowych.

2. W odniesieniu do zagadnień nieobjętych postanowieniami niniejszej Umowy, takich jak: odmowa wydania wizy, uznawanie dokumentów podróży, dowód posiadania wystarczających środków utrzymania, odmowa wjazdu oraz procedury wydalania osób, stosuje się prawo krajowe Ukrainy, prawo państw członkowskich bądź prawo Unii Europejskiej."

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiające Wspólnotowy Kodeks Wizowy (kodeks wizowy) (Dz.U. L 243 z 15.9.2009, s. 1).

Bez uszczerbku dla jej art. 10 (który przewiduje zwolnienie z obowiązku wizowego dla posiadaczy ukraińskich paszportów dyplomatycznych i służbowych paszportów biometrycznych), Umowa nie wpływa na obowiązujące przepisy dotyczące obowiązku wizowego lub zwolnienia z obowiązku wizowego. Na przykład, w art. 4 rozporządzenia Rady (WE) nr 539/2001 ([1]) zezwolono państwom członkowskim na zwolnienie z obowiązku wizowego między innymi cywilnych załóg samolotów i statków.

Przepisy Schengen oraz, w stosownych przypadkach, prawo krajowe mają nadal zastosowanie do zagadnień nieobjętych postanowieniami Umowy, takich jak: odmowa wydania wizy, uznanie dokumentów podróży, dowód posiadania wystarczających środków utrzymania, odmowa wjazdu oraz procedury wydalania osób. Odnosi się to również do przepisów Schengen dotyczących określania państwa członkowskiego strefy Schengen odpowiedzialnego za rozpatrzenie wniosku wizowego. W związku z tym obywatel Ukrainy powinien nadal ubiegać się o wizę w konsulacie państwa członkowskiego głównego celu podróży; natomiast jeżeli główny cel podróży nie jest określony, powinien zwrócić się do konsulatu państwa członkowskiego pierwszego wjazdu na obszar Schengen.

Nawet jeśli warunki przewidziane w Umowie zostały spełnione, np. wnioskodawca dostarczył dokumenty uzasadniające cel podróży w przypadku kategorii przewidzianych w art. 4, można nadal odmówić wydania wizy, jeżeli warunki ustanowione w art. 5 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 562/2006 ([2]) (zwanego dalej „kodeksem granicznym Schengen") nie zostały spełnione, tzn. osoba nie jest w posiadaniu ważnego dokumentu podróży, dokonano wpisu w SIS, osoba jest uważana za zagrożenie dla porządku publicznego, bezpieczeństwa wewnętrznego itp.

Inne możliwości w zakresie elastyczności w wydawaniu wiz dozwolone w kodeksie wizowym nadal obowiązują. Na przykład, wizy wielokrotnego wjazdu z długim okresem ważności – do pięciu lat- mogą być wydawane osobom innym niż osoby wymienione w art. 5 Umowy, jeżeli warunki przewidziane w kodeksie wizowym zostały spełnione (por. art. 24 ust. 2 kodeksu wizowego). W ten sam sposób nadal obowiązują przepisy zawarte w kodeksie wizowym umożliwiające zwolnienie z opłaty wizowej lub jej ograniczenie (zob. II. 2.1.1.).

1.3. **Rodzaje wiz objętych zakresem stosowania Umowy.**

W art. 3 lit. d) Umowy zdefiniowano „wizę" jako „zezwolenie wydane przez jedno z państw członkowskich lub decyzję podjętą przez takie państwo, które są wymagane w związku z:

— wjazdem na terytorium tego państwa członkowskiego lub kilku państw członkowskich z zamiarem pobytu nie dłuższego niż łącznie 90 dni,

— wjazdem w celu tranzytu przez terytorium tego państwa lub kilku państw członkowskich."

Następujące rodzaje wiz są objęte Umową:

— wizy kategorii „C" (wizy krótkoterminowe).

Ułatwienia przewidziane w Umowie mają zastosowanie zarówno do wiz jednolitych ważnych na całym terytorium państw członkowskich jak i do wiz o ograniczonej ważności terytorialnej.

1.4. **Obliczenia dotyczące długości pobytu, do jakiego uprawnia wiza, a w szczególności dotyczące ustalenia okresu sześciomiesięcznego.**

Niedawna modyfikacja kodeksu granicznego Schengen wprowadziła zmianę do pojęcia pobytu krótkoterminowego. Obecnie pobyt krótkoterminowy oznacza: „90 dni w każdym okresie 180-dniowym, co oznacza wzięcie pod uwagę okresu 180-dniowego poprzedzającego każdy z dni pobytu".

Data wjazdu liczona jest jako pierwszy dzień pobytu na terytorium państw członkowskich, a data wyjazdu liczona jest jako ostatni dzień pobytu na terytorium państw członkowskich. Pojęcie „każdy" oznacza stosowanie „ruchomego" 180-dniowego okresu odniesienia, zakładającego sprawdzenie dla każdego dnia pobytu okresu 180 dni wstecz w celu ustalenia, czy wymóg 90/180 dni został spełniony. Oznacza to, że nieobecność przez nieprzerwany okres 90 dni umożliwia kolejny pobyt przez okres do 90 dni.

Definicja ta weszła w życie w dniu 18 października 2013 r. Odpowiedni kalkulator można znaleźć na stronie: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm

([1]) Rozporządzenie Rady (WE) nr 539/2001 z dnia 15 marca 2001 r. wymieniające państwa trzecie, których obywatele muszą posiadać wizy podczas przekraczania granic zewnętrznych, oraz te, których obywatele są zwolnieni z tego wymogu (Dz.U. L 81 z 21.3.2001, s. 1).

([2]) Rozporządzenie (WE) nr 562/2006 Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. ustanawiające wspólnotowy kodeks zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.U. L 105 z 13.4.2006, s. 1).

Przykład obliczenia dni pobytu na podstawie nowej definicji:

Posiadacz rocznej wizy wielokrotnego wjazdu (18.4.2014 r. – 18.4.2015 r.) wjeżdża na terytorium państw członkowskich po raz pierwszy w dniu 19.4.2014 r. i pozostaje przez 3 dni. Kolejny raz wjeżdża na to terytorium w dniu 18.6.2014 r. i pozostaje przez 86 dni. Jak przedstawia się sytuacja w poszczególnych dniach? Kiedy osobie tej będzie wolno ponownie wjechać na terytorium państw członkowskich?

W dniu 11.9.2014 r.: W ciągu ostatnich 180 dni (16.3.2014 r.-11.9.2014 r.) dana osoba przebywała przez okres 3 dni (19. — 21.4.2014) plus 86 dni (18.6.2014 r. – 11.9.2014 r.) = 89 dni = nie przekroczono dozwolonego okresu pobytu. Dana osoba może pozostać jeszcze 1 dzień dłużej.

Od dnia 16.10.2014 r.: Osoba może wjechać na dodatkowe 3 dni (w dniu 16.10.2014 r. pobyt w dniu 19.4.2014 r. przestaje mieć znaczenie (wykracza poza okres 180 dni); w dniu 17.10.2014 r. pobyt w dniu 20.4.2014 r. przestaje mieć znaczenie (wykracza poza okres 180 dni; itd.).

Od dnia 15.12.2014 r.: Osoba ta może wjechać na 86 dodatkowych dni (w dniu 15.12.2014 r. pobyt z dnia 18.6.2014 przestaje mieć znaczenie (wykracza poza okres 180 dni); w dniu 16.12.2014 r., pobyt w dniu 19.6.2014 przestaje mieć znaczenie itd.).

1.5. **Sytuacja w odniesieniu do państw członkowskich, które jeszcze nie stosują w pełni dorobku Schengen, państw członkowskich, które nie uczestniczą we wspólnej polityce wizowej UE i krajów stowarzyszonych.**

Państwa członkowskie, które przystąpiły do Unii w 2004 r. (Republika Czeska, Estonia, Cypr, Łotwa, Litwa, Węgry, Malta, Polska, Słowenia i Słowacja), w 2007 r. (Bułgaria i Rumunia) i w 2013 (Chorwacja) są związane Umową od dnia jej wejścia w życie.

Jedynie, Bułgaria, Chorwacja, Cypr i Rumunia nie wprowadziły jeszcze w pełni przepisów dorobku Schengen. Będą one zatem nadal wydawać wizy krajowe, których ważność ograniczona jest do ich terytorium. W momencie wprowadzenia w pełni przez te państwa przepisów dorobku Schengen, będą one kontynuować stosowanie Umowy.

Prawo krajowe wciąż ma zastosowanie do wszystkich kwestii nieobjętych Umową do czasu pełnego wprowadzenia w życie dorobku Schengen przez te państwa członkowskie. Od tego dnia przepisy Schengen lub prawo krajowe mają zastosowanie do kwestii, które nie zostały uregulowane postanowieniami Umowy.

Bułgaria, Chorwacja, Cypr i Rumunia są upoważnione do uznawania dokumentów pobytowych, wiz kategorii „D" i wiz krótkoterminowych wydanych przez państwa Schengen i państwa stowarzyszone w przypadku pobytu krótkoterminowego na ich terytorium.

Zgodnie z art. 21 Konwencji wykonawczej do układu z Schengen z dnia 14 czerwca 1985 r. w sprawie stopniowego znoszenia kontroli na wspólnych granicach, wszystkie państwa Schengen muszą uznawać ważność wiz długoterminowych oraz dokumentów pobytowych wydanych przez organy innych państw Schengen w odniesieniu do pobytów krótkoterminowych na swoich terytoriach. Państwa członkowskie obszaru Schengen akceptują dokumenty pobytowe, wizy kategorii „D" i wizy krótkoterminowe krajów stowarzyszonych w zakresie wjazdu i pobytu krótkoterminowego i vice versa.

Umowa nie ma zastosowania do Danii, Irlandii i Zjednoczonego Królestwa ale zawiera wspólne deklaracje dotyczące woli tych państw członkowskich do zawarcia umów dwustronnych o ułatwieniach wizowych z Ukrainą.

Dwustronna Umowa o ułatwieniach wizowych pomiędzy Danią a Ukrainą weszła w życie z dniem 1 marca 2009 r. Negocjacje w sprawie ułatwień wizowych między Ukrainą a, odpowiednio, Irlandią i Zjednoczonym Królestwem nie miały jeszcze miejsca.

Mimo iż Islandia, Liechtenstein, Norwegia i Szwajcaria są krajami stowarzyszonymi Schengen, Umowa nie ma do nich zastosowania, ale zawiera wspólne deklaracje o woli tych państw do zawarcia umów dwustronnych o ułatwieniach wizowych z Ukrainą.

Norwegia podpisała dwustronną Umowę o ułatwieniach wizowych w dniu 13 lutego 2008 r. Umowa ta weszła w życie w dniu 1 września 2011 r.

Szwajcaria zakończyła negocjacje w sprawie podpisania dwustronnej Umowy o ułatwieniach wizowych w listopadzie 2011 r. Islandia podała do wiadomości, że rozpoczęła negocjacje z Ukrainą.

1.6. **Umowa/umowy dwustronne.**

Art. 13 ust. 1 Umowy stanowi:

„1. Od wejścia w życie niniejsza Umowa ma pierwszeństwo wobec postanowień umów lub ustaleń dwustronnych lub wielostronnych zawartych między poszczególnymi państwami członkowskimi a Ukrainą w zakresie, w jakim postanowienia tych umów i ustaleń dotyczą zagadnień objętych niniejszą Umową."

Od daty wejścia w życie Umowy postanowienia umów dwustronnych obowiązujących między państwami członkowskimi a Ukrainą w ramach kwestii objętych zakresem Umowy przestały obowiązywać. Zgodnie z prawem unijnym, państwa członkowskie są zobowiązane do podjęcia niezbędnych środków w celu wyeliminowania niezgodności między umowami dwustronnymi a Umową.

Jednakże art. 13 ust. 2 Umowy stanowi, że:

„2. Postanowienia umów dwustronnych lub ustaleń między poszczególnymi państwami członkowskimi a Ukrainą zawarte przed wejściem w życie niniejszej Umowy przewidującej zwolnienie posiadaczy służbowych paszportów nie biometrycznych z obowiązku wizowego mają zastosowanie bez uszczerbku dla prawa danych państw członkowskich lub Ukrainy do wypowiedzenia lub zawieszenia tych dwustronnych umów lub ustaleń."

Następujące państwa członkowskie zawarły umowy dwustronne z Ukrainą dotyczące zwolnienia z obowiązku wizowego dla posiadaczy paszportów służbowych: Bułgaria, Chorwacja, Cypr, Litwa, Łotwa, Polska, Rumunia, Słowacja i Węgry.

Zgodnie z art. 13 ust. 1 Umowy, w zakresie, w jakim umowy dwustronne te dotyczą posiadaczy biometrycznych paszportów służbowych, art. 10 ust. 2 Umowy ma pierwszeństwo nad postanowieniami tych umów dwustronnych. Zgodnie z art. 13 ust. 2 Umowy, postanowienia tych umów dwustronnych, które zostały zawarte przed wejściem w życie Umowy zmieniającej, mają nadal zastosowanie do posiadaczy nie biometrycznych paszportów służbowych, bez uszczerbku dla prawa danych państw członkowskich lub Ukrainy do wypowiedzenia lub zawieszenia tych dwustronnych umów lub ustaleń. Zwolnienie z obowiązku wizowego dla posiadaczy nie biometrycznych paszportów służbowych przyznane przez państwo członkowskie ma zastosowanie wyłącznie do terytorium tego państwa członkowskiego i nie dotyczy podróży na terytorium innych państw członkowskich należących do strefy Schengen.

Jeżeli państwo członkowskie zawarło dwustronną umowę lub porozumienie z Ukrainą w sprawie zagadnień nieobjętych Umową, zwolnienie takie będzie w dalszym ciągu obowiązywać po wejściu w życie Umowy.

1.7. **Deklaracja Wspólnoty Europejskiej dotycząca dostępu do misji dyplomatycznych i urzędów konsularnych przez osoby ubiegające się o wizę oraz harmonizacji informacji o procedurach wydawania wiz krótkoterminowych i dokumentach, jakie należy złożyć wraz z wnioskiem o wizę krótkoterminową.**

Zgodnie z deklaracją Wspólnoty Europejskiej załączoną do Umowy, przygotowano wspólne podstawowe informacje w sprawie dostępu osób ubiegających się o wizę do misji dyplomatycznych i urzędów konsularnych państw członkowskich oraz na temat procedur i warunków wydawania wiz oraz ich ważności w celu zapewnienia wnioskodawcom spójnych i jednolitych informacji. Informacje te są dostępne na stronie internetowej delegatury UE na Ukrainie: http://eeas.europa.eu/delegations/ukraine/index_en.htm

Misje dyplomatyczne oraz urzędy konsularne państw członkowskich proszone są o szerokie rozpowszechnianie tych informacji (na tablicach informacyjnych, ulotkach, na stronach internetowych itp.) oraz rozpowszechnianie również szczegółowych informacji na temat warunków wydawania wiz, reprezentacji państw członkowskich na Ukrainie i zharmonizowanego na szczeblu UE wykazu wymaganych dokumentów uzupełniających.

II. WYTYCZNE W SPRAWIE PRZEPISÓW SZCZEGÓLNYCH

2.1. **Przepisy, które mają zastosowanie do wszystkich osób ubiegających się o wizę**

Uwaga: Należy przypomnieć, że wymienione poniżej ułatwienia w odniesieniu do wizowej opłaty manipulacyjnej, czasu trwania procedur rozpatrywania wniosków wizowych, wyjazdu w przypadku zgubienia lub kradzieży dokumentów oraz przedłużenia okresu ważności wizy w wyjątkowych okolicznościach mają zastosowanie do wszystkich obywateli ukraińskich ubiegających się o wizę i posiadających wizy.

2.1.1. *Wizowa opłata manipulacyjna.*

Art. 6 ust. 1 Umowy stanowi:

„Opłata za rozpatrzenie wniosku wizowego złożonego przez obywatela ukraińskiego wynosi 35 EUR. Wyżej wymieniona kwota może ulec zmianie zgodnie z procedurą określoną w art. 14 ust. 4."

Zgodnie z art. 6 ust. 1, opłata za rozpatrzenie wniosku wizowego wynosi 35 EUR. Opłata ta będzie obowiązywać wszystkich obywateli ukraińskich ubiegających się o wizę (w tym turystów) i obejmie wizy krótkoterminowe, niezależnie od liczby wjazdów. Opłata ta ma również zastosowanie do wniosków wizowych składanych na granicach zewnętrznych.

Art. 6 ust. 2 Umowy stanowi:

„W przypadku ponownego wprowadzenia przez Ukrainę obowiązku wizowego dla obywateli UE opłata wizowa pobierana przez Ukrainę nie będzie przekraczała 35 EUR albo kwoty uzgodnionej w przypadku zmiany opłaty zgodnie z procedurą określoną w art. 14 ust. 4.".

Art. 6 ust. 3 Umowy stanowi:

„Państwa członkowskie pobierają opłatę w wysokości 70 EUR za rozpatrzenie wniosku wizowego w przypadku gdy, w oparciu o odległość między miejscem pobytu wnioskodawcy a miejscem złożenia wniosku, wnioskodawca zwrócił się o wydanie decyzji w sprawie wniosku w terminie trzech dni od jego złożenia, a placówka konsularna zgodziła się wydać decyzję w terminie trzech dni."

Opłatę w wysokości 70 EUR pobiera się za rozpatrzenie wniosku wizowego w przypadkach, gdy wniosek wizowy oraz dokumenty uzupełniające zostały złożone przez wnioskodawcę, którego miejsce pobytu znajduje się w obwodzie, w którym państwo członkowskie, do którego wnioskodawca planuje podróż, nie ma przedstawicielstwa konsularnego (jeżeli w tym obwodzie nie ma konsulatu, centrum wizowego, ani konsulatów państw członkowskich, które zawarły umowy o reprezentacji z tym państwem członkowskim, do którego wnioskodawca planuje podróż) oraz w przypadku gdy misja dyplomatyczna lub urząd konsularny zgodziły się na podjęcie decyzji w sprawie wniosku wizowego w ciągu trzech dni. Dokumenty poświadczające miejsce pobytu osoby składającej wniosek o wizę są wyszczególnione w formularzu wniosku wizowego.

Co do zasady, art. 6 ust. 3 Umowy ma na celu ułatwienie ubiegania się o wizę osobom, których miejsce zamieszkania znajduje się w dużej odległości od konsulatu. Jeżeli występuje konieczność odbycia długiej podróży w celu złożenia wniosku o wizę, dąży się do wydania jej szybko, tak by wnioskodawca mógł otrzymać wizę bez potrzeby odbycia tej samej długiej podróży po raz drugi.

Z wyżej wymienionych powodów, w przypadkach gdy „standardowy" czas rozpatrywania wniosku wizowego przez daną misję dyplomatyczną lub urząd konsularny wynosi trzy dni lub mniej, nalicza się standardową opłatę wizową w wysokości 35 EUR.

W przypadku misji dyplomatycznych i urzędów konsularnych, które dysponują systemem ustalania terminów spotkań, czas przeznaczony na umówienie takiego spotkania nie jest wliczany do okresu przetwarzania wniosku (zob. również II.2.1.2).

Art. 6 ust. 4 Umowy stanowi:

„4. Bez uszczerbku dla ust. 5 w odniesieniu do następujących kategorii osób odstępuje się od pobierania opłaty za rozpatrzenie wniosku wizowego:

a) osób bliskich – małżonków, dzieci (w tym przysposobionych), rodziców (w tym opiekunów), dziadków i wnuków – obywateli Ukrainy legalnie zamieszkujących na terytorium państw członkowskich lub obywateli Unii Europejskiej przebywających na terytorium państwa członkowskiego, którego są obywatelami;".

(Uwaga: Punkt ten reguluje sytuację ukraińskich bliskich krewnych podróżujących do państw członkowskich do obywateli Ukrainy legalnie zamieszkujących na terytorium państw członkowskich lub obywateli Unii Europejskiej zamieszkujących na terytorium państwa członkowskiego, którego są obywatelami. Obywatelom ukraińskim ubiegającym się o wizę, będącym członkami rodziny obywatela Unii w rozumieniu art. 5 ust. 2 dyrektywy Parlamentu Europejskiego i Rady 2004/38/WE [1], wizy są wydawane nieodpłatnie, tak szybko jak to możliwe, oraz na podstawie procedury przyspieszonej).

„b) członków oficjalnych delegacji, którzy na oficjalne zaproszenia skierowane do Ukrainy uczestniczą w spotkaniach, konsultacjach, negocjacjach lub programach wymiany, a także w wydarzeniach organizowanych na terytorium jednego z państw członkowskich przez organizacje międzyrządowe;

c) członków rządów i parlamentów krajowych i regionalnych oraz sądów konstytucyjnych i sądów najwyższych, w przypadku gdy nie są oni zwolnieni z obowiązku wizowego na mocy niniejszej Umowy;

d) uczniów, studentów, studentów studiów podyplomowych oraz towarzyszących im nauczycieli, którzy odbywają podróż w celu podjęcia nauki lub odbycia szkoleń;

e) osób niepełnosprawnych, i – jeśli to konieczne – ich opiekunów;" (Uwaga: w celu skorzystania ze zwolnienia z opłaty wizowej należy dostarczyć dokumenty potwierdzające, że każda z osób ubiegających się o wizę należy do tej kategorii).

„f) osób, które przedstawiły dowody potwierdzające konieczność wyjazdu z przyczyn humanitarnych, w tym w celu poddania się pilnemu zabiegowi medycznemu, oraz osób im towarzyszących, w celu udziału w pogrzebie osoby bliskiej albo w celu odwiedzenia ciężko chorej osoby bliskiej;

g) uczestników międzynarodowych imprez sportowych oraz osób im towarzyszących;" (Uwaga: Jedynie osoby towarzyszące podróżujące w ramach działalności zawodowej są objęte zwolnieniem; kibiców zatem nie uznaje się za osoby towarzyszące).

[1] Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.U. L 158 z 30.4.2004, s. 77).

„h) osób biorących udział w działaniach naukowych, kulturalnych i artystycznych, w tym programach uniwersyteckich i innych programach wymiany;

i) uczestników oficjalnych programów wymiany organizowanych przez miasta bliźniacze i inne podmioty komunalne;

j) dziennikarzy i członków personelu technicznego towarzyszących im w ramach swoich obowiązków zawodowych;" (Uwaga: zwolnieniem objęci są dziennikarze, do których zastosowanie ma art. 4 ust. 1 lit. e) Umowy).

„k) emerytów i rencistów;" (Uwaga: w celu skorzystania ze zwolnienia z opłaty wizowej w tej kategorii, osoby ubiegające się o wizę muszą przedstawić dokumenty potwierdzające status emeryta lub rencisty).

„l) kierowców przewożących towary w ruchu międzynarodowym i świadczących usługi transportu pasażerskiego, przemieszczających się na obszar państw członkowskich pojazdami zarejestrowanymi na Ukrainie;

m) członków załóg pociągów, wagonów chłodniczych i lokomotyw w pociągach międzynarodowych przemieszczających się na obszar państw członkowskich;

n) dzieci poniżej 18. roku życia oraz pozostających na utrzymaniu rodziców dzieci poniżej 21. roku życia." (Uwaga: w celu skorzystania ze zwolnienia z opłaty wizowej w tej kategorii, osoby ubiegające się o wizę muszą przedstawić dowody potwierdzające ich wiek; oraz – jeśli mają mniej niż 21 lat – dodatkowo dokument potwierdzający pozostawanie na utrzymaniu rodziców.);

„o) przedstawicieli wspólnot wyznaniowych;

p) przedstawicieli wolnych zawodów biorących udział w międzynarodowych wystawach, konferencjach, sympozjach, seminariach lub innych podobnych imprezach odbywających się na terytorium państw członkowskich;

q) osób w wieku do lat 25 uczestniczących w seminariach, konferencjach, imprezach sportowych, kulturalnych lub edukacyjnych organizowanych przez organizacje nienastawione na osiąganie zysku;

r) przedstawicieli organizacji społeczeństwa obywatelskiego odbywających podróże w celu udziału w szkoleniach, seminariach i konferencjach, w tym w ramach programów wymiany;

s) uczestników oficjalnych programów współpracy transgranicznej Unii Europejskiej, takich jak Europejski Instrument Sąsiedztwa i Partnerstwa (ENPI).

Akapit pierwszy stosuje się również, gdy celem podróży jest przejazd".

Art. 6 ust. 4 akapit drugi Umowy stosuje się tylko w przypadku, gdy cel podróży do państwa trzeciego jest równoważny z jednym z celów wymienionych w art. 6 ust. 4 lit. a) – s) Umowy, np. w sytuacji, gdy przejazd jest konieczny w celu wzięcia udziału w seminarium, odbycia wizyty u członków rodziny, uczestnictwa w programie wymiany organizacji społeczeństwa obywatelskiego itd. w państwie trzecim.

Osoby należące do wyżej wymienionych kategorii są całkowicie zwolnione z obowiązku uiszczenia opłaty wizowej. Ponadto, zgodnie z art. 16 ust. 6 kodeksu wizowego, „w indywidualnych przypadkach można odstąpić od poboru opłaty wizowej lub obniżyć jej wysokość, jeżeli służy to interesom kulturalnym lub sportowym, jak również interesom w dziedzinie polityki zagranicznej, polityki na rzecz rozwoju lub w innych dziedzinach ważnych z punktu widzenia interesu publicznego lub z przyczyn humanitarnych."

Jednakże zasada ta nie może być stosowana do odstąpienia od opłaty wizowej w wysokości 70 EUR za rozpatrzenie wizy w indywidualnych przypadkach, gdy wniosek wizowy oraz dokumenty uzupełniające zostały złożone przez wnioskodawcę, którego miejsce pobytu znajduje się w dużej odległości od misji dyplomatycznej lub urzędu konsularnego państwa członkowskiego i który należy do jednej kategorii osób zwolnionych z opłaty wizowej, wymienionych w art. 6 ust. 4 Umowy.

Należy również przypomnieć, że wnioskodawcy należący do kategorii osób zwolnionych z opłaty wizowej mogą nadal podlegać obowiązkowi uiszczenia opłaty za usługę w przypadku gdy państwo członkowskie współpracuje z zewnętrznym usługodawcą.

Art. 6 ust. 5 Umowy stanowi:

„5. Jeżeli państwo członkowskie współpracuje z usługodawcą zewnętrznym, mając na względzie wydawanie wiz, usługodawca zewnętrzny może pobrać opłatę administracyjną. Opłata ta jest proporcjonalna do kosztów ponoszonych przez usługodawcę zewnętrznego z tytułu wykonywania swoich zadań i nie przekracza 30 EUR. Dane państwo członkowskie utrzymuje możliwość składania wniosków przez wszystkich wnioskodawców bezpośrednio w swoich placówkach konsularnych. Gdy wymaga się, aby wnioskodawcy odbyli spotkanie w celu złożenia wniosku, co do zasady, spotkanie odbywa się w okresie dwóch tygodni od dnia, w którym wystąpiono o spotkanie."

Zachowanie możliwości składania przez wszystkie kategorie osób ubiegających się o wizę wniosków bezpośrednio w konsulacie, nie zaś za pośrednictwem usługodawcy zewnętrznego, oznacza, że należy zapewnić faktyczną możliwość wyboru między tymi dwoma opcjami. Dostęp bezpośredni nie musi zostać zorganizowany na identycznych lub podobnych warunkach, na jakich zapewniony jest dostęp do usługodawcy, jednak warunki te nie powinny w praktyce uniemożliwiać dostępu bezpośredniego. Można wprawdzie przyjąć, że czas oczekiwania na uzyskanie terminu spotkania będzie różnił się w przypadku dostępu bezpośredniego, jednak nie powinien być on tak długi, aby w praktyce sprawiał, że dostęp bezpośredni będzie niemożliwy.

2.1.2. *Czas trwania procedur rozpatrywania wniosków wizowych*

Art. 7 Umowy stanowi:

„1. Misje dyplomatyczne oraz urzędy konsularne państw członkowskich podejmują decyzję w sprawie wniosku o wydanie wizy w ciągu 10 dni kalendarzowych od dnia wpłynięcia wniosku i dokumentów wymaganych do wydania wizy.

2. W indywidualnych przypadkach, szczególnie w razie konieczności przeprowadzenia dokładniejszej analizy wniosku, okres na podjęcie decyzji w sprawie wniosku wizowego można przedłużyć do 30 dni kalendarzowych.

3. W nagłych przypadkach termin na podjęcie decyzji w sprawie wniosku wizowego można skrócić do dwóch dni roboczych lub mniej."

Decyzję w sprawie wniosku wizowego podejmuje się zasadniczo w ciągu 10 dni kalendarzowych od daty otrzymania kompletnego wniosku wizowego i dokumentów uzupełniających.

Okres ten może zostać przedłużony do 30 dni kalendarzowych, w przypadku gdy niezbędna jest dokładniejsza analiza wniosku – na przykład występuje konieczność konsultacji z organami centralnymi.

Bieg wszystkich wspomnianych terminów rozpoczyna się dopiero wtedy, gdy dokumentacja dołączona do wniosku jest kompletna, tj. od daty otrzymania wniosku wizowego i dokumentów uzupełniających.

W przypadku misji dyplomatycznych i urzędów konsularnych, dysponujących systemem umawiania spotkań, czas konieczny do ustalenia terminu spotkania nie jest zaliczany do okresu rozpatrywania wniosku. Podczas ustalania terminu spotkania należy wziąć pod uwagę możliwą potrzebę pilnego podjęcia decyzji zgłoszoną przez wnioskodawcę w celu zastosowania art. 7 ust. 3 Umowy. Co do zasady, spotkanie powinno się odbyć w okresie dwóch tygodni od daty złożenia wniosku o ustalenie terminu spotkania (por. art. 6 ust. 5 Umowy). Dłuższy okres powinien być wyjątkiem również w okresach szczególnego obciążenia pracą. Wspólny Komitet będzie uważnie monitorować tę sprawę. Państwa członkowskie starają się zapewnić, by spotkania na wniosek członków oficjalnych delegacji Ukrainy w celu złożenia wniosków w misjach dyplomatycznych i urzędach konsularnych następowały w pilnych przypadkach, gdy zaproszenie zostało wysłane z opóźnieniem, tak szybko, jak to możliwe, a najlepiej w terminie dwóch dni roboczych.

Urzędnik konsularny decyduje o skróceniu czasu na podjęcie decyzji w sprawie wniosku wizowego zgodnie z definicją w art. 7 ust. 3 Umowy.

2.1.3. *Przedłużenie okresu ważności wizy w wyjątkowych okolicznościach.*

Art. 9 Umowy stanowi:

„Obywatelom Ukrainy, którzy nie mogą opuścić terytorium państwa członkowskiego w terminie określonym w wizie z powodów związanych z działaniem siły wyższej, bezpłatnie przedłuża się wizę zgodnie z przepisami państwa przyjmującego na okres konieczny do powrotu do państwa zamieszkania."

W odniesieniu do możliwości przedłużenia ważności wizy w przypadkach wystąpienia siły wyższej – na przykład pozostania w szpitalu z powodu nieprzewidzianych okoliczności/nagłej choroby/wypadku – w przypadku gdy posiadacz wizy nie ma możliwości opuszczenia terytorium państwa członkowskiego przez datą określoną w jego wizie, zastosowanie mają przepisy art. 33 ust. 1 kodeksu wizowego, jeżeli są one zgodne z Umową (na przykład, przedłużona wiza pozostaje nadal wizą jednolitą, uprawniającą do wjazdu na terytorium wszystkich państw członkowskich obszaru Schengen, w odniesieniu do których obowiązywała w momencie wydania). Jednakże na mocy Umowy w przypadku działania siły wyższej przedłużenie ważności wizy odbywa się bezpłatnie.

2.2. **Zasady, które mają zastosowanie do niektórych kategorii osób ubiegających się o wizę.**

2.2.1. *Dokumenty potwierdzające cel podróży.*

W przypadku wszystkich kategorii osób wymienionych w art. 4 ust. 1 Umowy, w tym kierowców przewożących towary w ruchu międzynarodowym i świadczących usługi transportu pasażerskiego, w odniesieniu do celu podróży wymagane są wyłącznie wskazane/wymienione dokumenty potwierdzające. Od wnioskodawców należących do tych kategorii nie wymaga się żadnych innych dokumentów dotyczących celu pobytu. Jak stwierdzono w art. 4 ust. 3 Umowy, nie wymaga się żadnego innego uzasadnienia, zaproszenia lub potwierdzenia celu podróży.

Jeśli w poszczególnych przypadkach pojawią się wątpliwości co do rzeczywistego celu podróży, osoba ubiegająca się o wizę proszona jest o stawienie się na (dodatkową) szczegółową rozmowę w ambasadzie/konsulacie, tematem której może być rzeczywisty cel podróży lub też kwestia istnienia u wnioskodawcy zamiaru powrotu – por. art. 21 ust. 8 kodeksu wizowego. W takich indywidualnych przypadkach, osoba ubiegająca się o wizę może przedstawić dodatkowe dokumenty, lub też ich dostarczenia może – w drodze wyjątku – zażądać urzędnik konsularny. Wspólny Komitet będzie ściśle monitorować tę kwestię.

W przypadku osób należących do kategorii niewymienionych w art. 4 ust. 1 Umowy, nadal stosuje się obowiązujące przepisy dotyczące dokumentów potwierdzających cel podróży. To samo odnosi się do dokumentów dotyczących zgody rodziców na podróże dzieci poniżej 18 roku życia.

Przepisy Schengen lub prawo krajowe stosuje się do zagadnień nieobjętych postanowieniami niniejszej Umowy, takich jak uznawanie dokumentów podróży, podróżnego ubezpieczenia medycznego i gwarancji odnośnie do powrotu i wystarczających środków utrzymania (por. wyżej I.1.2.).

Zgodnie z „Deklaracją Unii Europejskiej dotyczącą dokumentów, które należy złożyć z wnioskiem o wizę krótkoterminową", załączoną do Umowy zmieniającej, „Unia Europejska ustanowi zharmonizowaną listę dokumentów uzupełniających, zgodnie z art. 48 ust. 1 lit. a) kodeksu wizowego, celem zapewnienia, by wnioskodawcy z Ukrainy byli zobowiązani do składania, co do zasady, takich samych dokumentów uzupełniających"; Konsulaty państw członkowskich, w ramach lokalnej współpracy schengeńskiej, proszone są o zapewnienie obywatelom ukraińskim ubiegającym się o wizę spójnych i jednolitych informacji podstawowych oraz stosowanie wobec nich wymogu składania zasadniczo tych samych dokumentów uzupełniających bez względu na konsulat państwa członkowskiego, który otrzyma wniosek wizowy.

Co do zasady, wraz z wnioskiem wizowym należy złożyć oryginał wniosku lub zaświadczenia dotyczącego dokumentu wymaganego na mocy art. 4 ust. 1 Umowy. Jednakże pracownicy konsulatu mogą rozpocząć rozpatrywanie wniosku wizowego na podstawie kopii wniosku lub zaświadczenia dotyczącego dokumentu. Niemniej jednak konsulat może zażądać przedłożenia oryginału dokumentu w przypadku pierwszego wniosku i jak również w przypadkach indywidualnych, co do których istnieją wątpliwości.

Jako że umieszczony poniżej wykaz organów zawiera niekiedy nazwisko osoby, która ma prawo zatwierdzać odpowiednie wnioski/certyfikaty, władze Ukrainy powinny informować lokalną współpracę schengeńską w momencie zastąpienia tej osoby na jej stanowisku.

Art. 4 Umowy stwierdza, że:

„1. W odniesieniu do niżej wymienionych kategorii obywateli Ukrainy za wystarczające uznaje się następujące dokumenty uzasadniające cel podróży na terytorium drugiej Strony:

a) w przypadku członków oficjalnych delegacji, którzy na oficjalne zaproszenia skierowane do Ukrainy uczestniczą w spotkaniach, konsultacjach, negocjacjach lub programach wymiany, a także w wydarzeniach organizowanych na terytorium jednego z państw członkowskich przez organizacje międzyrządowe:

— pismo wydane przez organ ukraiński potwierdzające, że wnioskodawca jest członkiem delegacji udającej się na terytorium drugiej Strony w celu udziału w jednym z wyżej wymienionych wydarzeń, wraz z kopią oficjalnego zaproszenia;"

Nazwisko osoby ubiegającej się o wizę musi być podane w piśmie wydanym przez właściwy organ, potwierdzającym, że ta osoba jest członkiem delegacji udającej się na terytorium drugiej Strony w celu wzięcia udziału w oficjalnym spotkaniu. Nie jest konieczne podawanie imienia i nazwiska wnioskodawcy w oficjalnym zaproszeniu do udziału w spotkaniu, chociaż może to mieć miejsce w przypadku, w którym oficjalne zaproszenie jest skierowane do konkretnych osób.

Przepis ten ma zastosowanie do członków oficjalnych delegacji, niezależnie od rodzaju paszportu, jakim dysponują (nie biometryczny paszport służbowy lub paszport zwykły).

„b) w przypadku przedsiębiorców i przedstawicieli organizacji przedsiębiorców:

— pisemny wniosek sporządzony przez przyjmującą osobę prawną, przedsiębiorstwo przyjmujące, biuro bądź oddział takiej osoby prawnej lub przedsiębiorstwa, władze państwowe lub lokalne państw członkowskich lub komitety organizacyjne targów, wystaw, konferencji i sympozjów handlowych mających miejsce na terytorium państw członkowskich;

c) w przypadku kierowców przewożących towary w ruchu międzynarodowym i świadczących usługi transportu pasażerskiego i przemieszczających się na obszar państw członkowskich pojazdami zarejestrowanymi na Ukrainie:

— w przypadku kierowców przewożących towary w ruchu międzynarodowym i świadczących usługi transportu pasażerskiego i przemieszczających się na obszar państw członkowskich pojazdami zarejestrowanymi na Ukrainie;"

Właściwe organy, które określają zasady dotyczące międzynarodowego transportu drogowego i odpowiadają za określenie celu, czasu trwania, miejsca podróży oraz częstotliwości przejazdów kierowców przewożących towary w ruchu międzynarodowym i świadczących usługi transportu pasażerskiego, przemieszczających się na obszar państw członkowskich pojazdami zarejestrowanymi na Ukrainie, to:

1. Zrzeszenie Międzynarodowych Przewoźników Drogowych Ukrainy (AsMAP/„АсМАП")

   Adres pocztowy AsMAP:

   ul. Szorsa 11

   Kijów, 03150, Ukraina

   Urzędnicy uprawnieni do zatwierdzania wniosków:

   Kostiuszenko Leonid – przewodniczący AsMAP Ukrainy;

   Dokil' Leonid – wiceprzewodniczący AsMAP Ukrainy;

   Kuszynskij Jurij – wiceprzewodniczący AsMAP Ukrainy.

2. Przedsiębiorstwo państwowe „Usługi międzynarodowego przewozu drogowego" (SE „SIRC")

   Adres pocztowy SE „SIRC":

   Prospekt Nauki 57

   Kijów, 03083, Ukraina

   Tel. +38 044 524 21 01

   Faks: +38 044 524 00 70

   Urzędnicy uprawnieni do zatwierdzania wniosków:

   Tkaczenko Anatolij – dyrektor SE „SIRC";

   Neronow Oleksandr – pierwszy zastępca dyrektora SE „SIRC".

3. Ukraiński związek transportu drogowego i logistyki

   Adres pocztowy Ukraińskiego związku transportu drogowego i logistyki:

   Ul. Predslawinska 28

   Kijów, 03150, Ukraina

   Tel./faks +38 044 528 71 30/+38 044 528 71 46/+38 044 529 44 40

   Urzędnik uprawniony do zatwierdzania wniosków:

   Lipowskij Vitalij – przewodniczący związku

4. Ogólnoukraińskie stowarzyszenie przewoźników samochodowych (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   Adres pocztowy AAAC:

   ul. Wełyka Wasylkiwśka 139

   Kijów, 03150, Ukraina

   Tel./faks: +38044-538-75-05, +38044-529-25-21

   Urzędnicy uprawnieni do zatwierdzania wniosków:

   Rewa Vitalij (Віталій Рева) – przewodniczący AAAC

   Gławatskij Petro (Петро Главатський) – wiceprzewodniczący AAAC

   e-mail: vaap@i.com.ua

5. Ogólnoukraińskie stowarzyszenie przewoźników samochodowych (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   Adres pocztowy AAAC:

   ul. Raisy Okipnoji 3,

   Kijów, 02002, Ukraina

   Tel./faks: +38044-517-44-31, +38044-516-47-26

   Urzędnicy uprawnieni do zatwierdzania wniosków:

   Wakulenko Wołodimir (Вакуленко Володимир Михайлович) – wiceprzewodniczący AAAC

6. Ukraińskie przedsiębiorstwo państwowe „Ukrinteravtoservice" (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів „Укрінтеравтосервіс")

   Adres pocztowy ukraińskiego przedsiębiorstwa państwowego „Ukrinteravtoservice":

   Prospekt Nauki 57,

   Kijów, 03083, Ukraina

   Urzędnicy uprawnieni do zatwierdzania wniosków:

   Dobrohod Sergij (Доброход Сергій Олександрович) – dyrektor generalny ukraińskiego przedsiębiorstwa państwowego „Ukrinteravtservice" (tel. +38 044 524 -09 -99 tel. kom.: +38 050 463 -89 -32)

   Kubalska Switłana (Кубальська Світлана Сергіївна) – zastępca dyrektora generalnego ukraińskiego przedsiębiorstwa państwowego „Ukrinteravtservice" (tel. +38 044 524 -09 -99 tel. kom.: +38 050 550 -82 -62)

Ze względu na obecne problemy związane z tą kategorią osób ubiegających się o wizę Wspólny Komitet będzie uważnie kontrolował wykonywanie tego przepisu.

„d) w przypadku członków załóg pociągów, wagonów chłodniczych i lokomotyw w pociągach międzynarodowych przemieszczających się na obszar państw członkowskich:

— pisemny wniosek sporządzony przez właściwe ukraińskie przedsiębiorstwo kolejowe określający cel, czas trwania i częstotliwość przejazdów;"

Właściwym organem w dziedzinie transportu kolejowego Ukrainy jest Państwowy Urząd Transportu Kolejowego Ukrainy („Ukrzaliznycja"/„Укрзалізниця").

Adres pocztowy „Ukrzaliznycji":

Ul. Twerskaja 5-7
Kijów, 03680, Ukraina

Zgodnie z podziałem kompetencji w kierownictwie „Ukrzaliznycji", urzędnikami odpowiedzialnymi za dostarczanie informacji dotyczących celu, czasu trwania i częstotliwości przejazdów członków załóg pociągów, wagonów chłodniczych i lokomotyw w pociągach międzynarodowych przemieszczających się na obszar państw członkowskich są:

Bołobolin Sergij (Болоболін Сергій Петрович) – pierwszy dyrektor generalny Ukrzaliznycji (tel. +38 044 465 00 10)

Sergijenko Mikoła (Сергієнко Микола Іванович) – pierwszy zastępca dyrektora generalnego Ukrzaliznycji (tel. +38 044 465 00 01)

Żurakiwskij Witalij (Жураківський Віталій Олександрович) – pierwszy zastępca dyrektora generalnego Ukrzaliznycji (tel. +38 044 465 00 41)

Slipczenko Oleksij (Сліпченко Олексій Леонтійович) – zastępca dyrektora generalnego Ukrzaliznycji (tel. +38 044 465 00 14)

Naumenko Petro (Науменко Петро Петрович) –zastępca dyrektora generalnego Ukrzaliznycji (tel. +38 044 465 00 12)

Czekałow Pawło (Чекалов Павло Леонтійович) – zastępca dyrektora generalnego Ukrzaliznycji (tel. +38 044 465 00 13)

Matwiiw Igor – kierownik departamentu stosunków międzynarodowych Ukrzaliznycji (tel. +38 044 465 04 25)

„e) w przypadku dziennikarzy i członków personelu technicznego towarzyszącego im w celach zawodowych:

— zaświadczenie lub inny dokument wydany przez organizację zawodową lub przez pracodawcę wnioskodawcy, stanowiące dowód, że dana osoba jest dziennikarzem zawodowym, oraz zaświadczające, że cel podróży wiąże się z zadaniem dziennikarskim, lub stanowiące dowód, że dana osoba jest członkiem personelu technicznego towarzyszącym dziennikarzowi w ramach swoich obowiązków zawodowych;"

Kategoria ta nie obejmuje dziennikarzy pracujących jako wolni strzelcy.

Konieczne jest przedłożenie zaświadczenia lub innego dokumentu stanowiącego dowód na to, że dana osoba jest zawodowym dziennikarzem i oryginału dokumentu wydanego przez pracodawcę osoby ubiegającej się o wizę, zaświadczającego, że cel podróży wiąże się z zadaniem dziennikarskim, lub stanowiącego dowód na to, że dana osoba jest członkiem ekipy technicznej towarzyszącej dziennikarzowi w celach zawodowych.

Właściwa ukraińska organizacja zawodowa, wydająca zaświadczenia zawodowym dziennikarzom:

1. Krajowy Związek Dziennikarzy Ukrainy (KZDU) („Національна спілка журналістів України", НСЖУ).

   KZDU wydaje wykwalifikowanym pracownikom środków masowego przekazu krajowe i międzynarodowe legitymacje dziennikarskie według standardowego wzoru określonego przez Międzynarodową Federację Dziennikarzy.

   Adres pocztowy KZDU:

   ul. Chreszczatyk 27-a

   Kijów, 01001, Ukraina

   Osoba upoważniona w ramach KZDU:

   Naliwajko Oleg Igorowicz (Наливайко Oleg Ігорович) – kierownik KZDU

   Tel./faks: +38044-234-20-96; +38044-234-49-60; +38044-234-52-09

   e-mail: spilka@nsju.org; admin@nsju.org.

2. Związek Niezależnych Mediów Ukrainy (ZNMU) („Незалежна медіа-профспілка України").

   Adres pocztowy ZNMU:

   Biuro 25

   Ul. Chreszczatyk 27-A

   Kijów, 01001, Ukraina

   Upoważnione osoby:

   Łukanow Jurij (Луканов Юрій Вадимович) – kierownik ZNMU

   Winniczuk Oksana (Оксана Винничук) – sekretarz wykonawczy ZNMU

   tel. +38 050 356 57 58

   e-mail: secretar@profspilka.org.ua

„f) w przypadku osób biorących udział w działaniach naukowych, kulturalnych i artystycznych, w tym programach uniwersyteckich i innych programach wymiany:

— pisemny wniosek sporządzony przez organizację przyjmującą uczestnika tych działań;

g) w przypadku uczniów, studentów, studentów podyplomowych oraz towarzyszących im nauczycieli, którzy odbywają podróż w celu podjęcia nauki lub odbycia szkoleń, w tym w ramach programów wymiany oraz innych działań szkolnych:

— pisemny wniosek lub zaświadczenie o wpisaniu na listę uczniów/studentów, sporządzone przez przyjmujące placówki: uniwersytet lub szkołę, lub legitymacja uczniowska/studencka bądź zaświadczenie o kursach, w których uczestniczyć będzie dana osoba;"

Legitymację studencką można uznać za uzasadnienie celu podróży jedynie w przypadku, jeżeli została wystawiona przez przyjmujący uniwersytet, kolegium lub szkołę, w których mają odbywać się studia lub szkolenie.

„h) w przypadku uczestników międzynarodowych imprez sportowych i osób towarzyszących im zawodowo:

— pisemny wniosek sporządzony przez organizację przyjmującą: właściwe organy, krajowe związki sportowe i krajowe komitety olimpijskie państw członkowskich;"

Wykaz osób towarzyszących w przypadku międzynarodowych imprez sportowych zostanie ograniczony do osób towarzyszących sportowcom zawodowo: trenerów, masażystów, menadżerów, personelu medycznego oraz szefa klubu sportowego. Kibiców nie uznaje się za osoby towarzyszące.

„i) w przypadku uczestników oficjalnych programów wymiany organizowanych przez miasta partnerskie i inne podmioty komunalne:

— pisemny wniosek sporządzony przez kierowników jednostek administracji/burmistrzów tych miast lub innych podmiotów komunalnych;"

Kierownik działu administracji/burmistrz miasta lub inny organ gminy właściwy do wydania pisemnego wniosku to kierownik działu administracji/burmistrz miasta przyjmującego lub gminy, na terenie których mają się odbyć działania w ramach partnerstwa. Kategoria ta obejmuje jedynie uznane programy partnerstwa.

„j) w przypadku bliskich krewnych – małżonków, dzieci (w tym przysposobionych), rodziców (w tym opiekunów), dziadków i wnuków – odwiedzających obywateli ukraińskich legalnie zamieszkujących na terytorium państw członkowskich lub obywateli Unii Europejskiej zamieszkujących na terytorium państwa członkowskiego, którego są obywatelami:

— pisemny wniosek sporządzony przez osobę przyjmującą;";

Litera ta reguluje sytuację ukraińskich bliskich krewnych podróżujących do państw członkowskich do obywateli Ukrainy legalnie zamieszkujących na terytorium państw członkowskich lub obywateli Unii Europejskiej zamieszkujących na terytorium państwa członkowskiego, którego są obywatelami.

Autentyczność podpisu osoby zapraszającej musi zostać potwierdzona przez właściwy organ zgodnie z przepisami krajowymi państwa zamieszkania.

Niezbędne jest również udowodnienie legalnego pobytu osoby zapraszającej i więzów rodzinnych; na przykład przedłożenie – wraz z pisemnym wnioskiem osoby przyjmującej – kopii dokumentów wskazujących na status danej osoby, takich jak fotokopie dokumentu pobytowego, oraz potwierdzających więzy rodzinne.

Przepis ten ma również zastosowanie do członków rodziny pracowników zatrudnionych w misjach dyplomatycznych i konsulatach przebywających w celu złożenia wizyty rodzinnej do 90 dni na terytorium państw członkowskich z wyjątkiem konieczności przedłożenia dowodu legalnego pobytu i więzów rodzinnych.

Zgodnie z deklaracją Unii Europejskiej w sprawie ułatwień dla członków rodzin, załączonej do Umowy zmieniającej: „Aby ułatwić przemieszczanie się większej liczbie osób powiązanych więzami rodzinnymi (w szczególności siostrom, braciom i ich dzieciom) z obywatelami Ukrainy legalnie zamieszkującymi na terytorium państw członkowskich lub obywatelami Unii Europejskiej, Unia Europejska zwraca się do placówek konsularnych państw członkowskich o pełne korzystanie z przewidzianych w kodeksie wizowym możliwości zapewnienia ułatwień w wydawaniu wiz takim osobom, w szczególności poprzez ograniczenie liczby dokumentów wymaganych od wnioskodawców, zwolnienie z opłat manipulacyjnych i w stosownych przypadkach wydawanie wiz wielokrotnego wjazdu."

„k) w przypadku osób bliskich wyjeżdżających w związku z ceremoniami pogrzebowymi:

— oficjalny dokument potwierdzający fakt zgonu, jak również poświadczenie pokrewieństwa lub innego związku łączącego wnioskodawcę ze zmarłym;"

Umowa nie precyzuje, które organy powinny wydać wspomniany wyżej oficjalny dokument: czy organy państwa, w którym odbędzie się ceremonia pogrzebowa, czy organy państwa, w którym zamieszkuje osoba pragnąca wziąć udział w ceremonii pogrzebowej. Należy przyjąć, iż właściwe organy obu państw mogą wydać taki oficjalny dokument.

Należy przedstawić wspomniany wyżej oficjalny dokument potwierdzający fakt zgonu oraz poświadczenie pokrewieństwa lub innego związku łączącego wnioskodawcę ze zmarłym, np. akt urodzenia lub małżeństwa.

„l) w przypadku osób pragnących odwiedzić cmentarz wojskowy lub cywilny:

— oficjalny dokument potwierdzający istnienie i fakt utrzymywania grobu, a także pokrewieństwo lub inny związek łączący wnioskodawcę z pochowanym;"

Umowa nie określa szczegółowo, czy wspomniany powyżej oficjalny dokument powinien zostać wydany przez organy państwa, w którym znajduje się cmentarz czy też organy państwa, w którym zamieszkuje osoba pragnąca odwiedzić cmentarz. Należy przyjąć, iż właściwe organy obu państw mogą wydać taki oficjalny dokument.

Wspomniany wyżej oficjalny dokument potwierdzający istnienie i fakt utrzymywania grobu oraz pokrewieństwo lub inny związek łączący osobę ubiegającą się o wizę z pochowanym musi zostać przedstawiony.

Zgodnie z deklaracją Wspólnoty Europejskiej dotyczącą wydawania wiz krótkoterminowych osobom pragnącym odwiedzić cmentarz wojskowy lub cywilny załączoną do Umowy, co do ogólnej zasady, wizy krótkoterminowe dla osób pragnących odwiedzić cmentarz wojskowy lub cywilny wydaje się na okres nie dłuższy niż 14 dni.

„m) w przypadku osób podróżujących z powodów zdrowotnych i niezbędnych osób towarzyszących:

— dokument urzędowy wystawiony przez daną instytucję medyczną, poświadczający konieczność objęcia danej osoby opieką medyczną w tej instytucji, konieczność obecności osoby towarzyszącej oraz dowód posiadania wystarczających środków finansowych na pokrycie kosztów leczenia".

Należy przedstawić dokument wystawiony przez daną instytucję medyczną, poświadczający konieczność objęcia danej osoby opieką medyczną w tej instytucji oraz dowód posiadania środków finansowych wystarczających na pokrycie kosztów leczenia, który powinien również potwierdzać konieczność obecności osoby towarzyszącej.

„n) w przypadku przedstawicieli organizacji społeczeństwa obywatelskiego odbywających podróże w celu udziału w szkoleniach, seminariach i konferencjach, w tym w ramach programów wymiany:

— pisemny wniosek wydany przez organizację przyjmującą, zaświadczenie potwierdzające, że dana osoba reprezentuje organizację społeczeństwa obywatelskiego i zaświadczenie o założeniu takiej organizacji z odpowiedniego rejestru, sporządzone przez organ państwowy zgodnie z ustawodawstwem krajowym;"

Dokumentem potwierdzającym rejestrację organizacji społeczeństwa obywatelskiego na Ukrainie jest pismo Państwowej Służby Rejestracyjnej Ukrainy zawierające informacje z rejestru stowarzyszeń publicznych.

„o) w przypadku przedstawicieli wolnych zawodów biorących udział w międzynarodowych wystawach, konferencjach, sympozjach, seminariach lub innych podobnych imprezach odbywających się na terytorium państw członkowskich:

— pisemny wniosek sporządzony przez organizację przyjmującą, potwierdzający udział danej osoby w imprezie;

p) w przypadku przedstawicieli wspólnot wyznaniowych:

— pisemny wniosek sporządzony przez wspólnotę wyznaniową zarejestrowaną na Ukrainie, określający cel, czas trwania i częstotliwość przejazdów;"

Dokumentem potwierdzającym rejestrację wspólnoty religijnej na Ukrainie jest wyciąg z Jednolitego Państwowego Rejestru Osób Prawnych i Osób Fizycznych – Przedsiębiorców zawierający informację, że organizacyjną i prawną postacią osoby prawnej jest wspólnota religijna.

„q) w przypadku uczestników oficjalnych programów współpracy transgranicznej Unii Europejskiej, takich jak Europejski Instrument Sąsiedztwa i Partnerstwa (ENPI):

— pisemny wniosek sporządzony przez organizację przyjmującą."

Uwaga: Umowa nie tworzy żadnych nowych przepisów dotyczących odpowiedzialności w odniesieniu do osób fizycznych lub prawnych wydających pisemne wnioski. W odniesieniu do sfałszowanych wniosków zastosowanie mają odpowiednie przepisy krajowe/unijne.

2.2.2. *Wydawanie wiz wielokrotnego wjazdu.*

W przypadkach, gdy osoba ubiegająca się o wizę jest zmuszona do częstego lub regularnego podróżowania na terytorium państw członkowskich, wydaje się wizy krótkoterminowe na kilka wizyt, pod warunkiem że łączny czas trwania tych wizyt nie przekracza 90 dni w ciągu każdego 180-dniowego okresu.

Art. 5 ust. 1 Umowy stanowi:

„1. Misje dyplomatyczne oraz urzędy konsularne państw członkowskich wydają wizy wielokrotnego wjazdu o pięcioletnim okresie ważności następującym kategoriom osób:

a) członkom rządów i parlamentów krajowych i regionalnych oraz trybunałów konstytucyjnych i sądów najwyższych, prokuratorom na szczeblu krajowym i regionalnym oraz ich zastępcom, o ile nie są oni zwolnieni z obowiązku wizowego na mocy niniejszej Umowy, w zakresie pełnionych przez nich obowiązków;

b) stałym członkom oficjalnych delegacji, którzy na oficjalne zaproszenia skierowane do Ukrainy uczestniczą regularnie w spotkaniach, konsultacjach, negocjacjach lub programach wymiany, a także w wydarzeniach organizowanych na terytorium państw członkowskich przez organizacje międzyrządowe;

c) małżonkom i dzieciom (w tym przysposobionym) poniżej 21. roku życia lub pozostających na utrzymaniu rodziców oraz rodzicom (w tym opiekunom) odwiedzającym obywateli Ukrainy zamieszkujących legalnie na terytorium państw członkowskich lub obywateli Unii Europejskiej przebywających na terytorium państwa członkowskiego, którego są obywatelami;

d) przedsiębiorcom i przedstawicielom organizacji branżowych, którzy odbywają regularne podróże do państw członkowskich;

e) dziennikarzom i członkom personelu technicznego towarzyszącym im w ramach swoich obowiązków zawodowych.

Na zasadzie odstępstwa od akapitu pierwszego, jeżeli konieczność lub zamiar częstego lub regularnego odbywania podróży są wyraźnie ograniczone do krótszego okresu, okres ważności wizy wielokrotnego wjazdu będzie ograniczony do tego okresu, w szczególności w przypadku:

— osób, o których mowa w lit. a), do okresu kadencji,

— osób, o których mowa w lit. b), do okresu ważności statusu stałego członka oficjalnej delegacji,

— osób, o których mowa w lit. c), do okresu ważności, na który zatwierdzono legalny pobyt obywateli Ukrainy, którzy przebywają legalnie w Unii Europejskiej,

— osób, o których mowa w lit. d), do okresu ważności statusu przedstawiciela podmiotu gospodarczego lub umowy o pracę,

— osób, o których mowa w lit. e), gdy okres na który zawarta została umowa o pracę

jest krótszy niż pięć lat.".

W odniesieniu do tych kategorii osób, biorąc pod uwagę ich status zawodowy lub związek rodzinny z obywatelem Ukrainy legalnie zamieszkującym na terytorium państw członkowskich lub obywatelem Unii Europejskiej zamieszkującym na terytorium państwa członkowskiego, którego jest obywatelem, uzasadnione jest, co do zasady, wydawanie wizy wielokrotnego wjazdu o pięcioletnim okresie ważności. W początkowej wersji Umowy wyrażenie „o okresie ważności co najwyżej pięciu lat" pozostawiało konsulatom swobodę przy podejmowaniu decyzji w sprawie okresu ważności wizy, określając wyłącznie maksymalny okres ważności. W Umowie zmieniającej swoboda ta zniknęła wraz z wprowadzeniem nowego sformułowania „o pięcioletnim okresie ważności", na podstawie którego, jeżeli wnioskodawca spełnia wszystkie wymogi art. 5 ust. 1 Umowy „Misje dyplomatyczne oraz urzędy konsularne państw członkowskich wydają wizy wielokrotnego wjazdu o pięcioletnim okresie ważności".

W przypadku osób objętych zakresem stosowania art. 5 ust. 1 lit. a) Umowy, należy dostarczyć potwierdzenie statusu zawodowego i okresu kadencji.

Przepis ten nie ma zastosowania do osób objętych zakresem stosowania art. 5 ust. 1 lit. a) Umowy, jeżeli są one zwolnione z obowiązku wizowego na mocy Umowy, tzn. jeśli są one posiadaczami paszportów dyplomatycznych lub biometrycznych paszportów służbowych.

W przypadku osób objętych zakresem stosowania art. 5 ust. 1 lit. b) Umowy, należy przedstawić dowód statusu stałego członka oficjalnej delegacji i potwierdzenie konieczności regularnego uczestnictwa w spotkaniach, konsultacjach, negocjacjach lub programach wymiany.

W przypadku osób objętych zakresem stosowania art. 5 ust. 1 lit. c) Umowy, należy przedstawić dowód potwierdzający legalny pobyt osoby zapraszającej (por. powyżej II.2.2.1).

W przypadku osób objętych zakresem stosowania art. 5 ust. 1 lit. d) i e), należy przedstawić dowód statusu zawodowego oraz okresu prowadzenia działalności.

Art. 5 ust. 2 Umowy stwierdza, że:

„2. Misje dyplomatyczne oraz służby konsularne państw członkowskich wydają wizy wielokrotnego wjazdu o jednorocznym okresie ważności następującym kategoriom osób, pod warunkiem że w poprzednim roku takie osoby otrzymały przynajmniej jedną wizę, z której skorzystały zgodnie z przepisami dotyczącymi wjazdu do danego kraju i pobytu w nim:

a) kierowcy przewożący towary w ruchu międzynarodowym i świadczący usługi transportu pasażerskiego i przemieszczający się na obszar państw członkowskich pojazdami zarejestrowanymi na Ukrainie;

b) członkowie załóg pociągów, wagonów chłodniczych i lokomotyw w pociągach międzynarodowych przemieszczających się na obszar państw członkowskich;

c) osoby biorące udział w działaniach naukowych, kulturalnych i artystycznych, w tym programach uniwersyteckich i innych programach wymiany, które odbywają regularne podróże do państw członkowskich;

d) uczestnicy międzynarodowych imprez sportowych i osoby im towarzyszące w celach zawodowych;

e) uczestnicy oficjalnych programów wymiany organizowanych przez miasta partnerskie i inne podmioty komunalne;

f) przedstawiciele organizacji społeczeństwa obywatelskiego odbywający regularne podróże do państw członkowskich w celu udziału w szkoleniach, seminariach i konferencjach, w tym w ramach programów wymiany;

g) uczestnicy oficjalnych programów współpracy transgranicznej Unii Europejskiej, takich jak Europejski Instrument Sąsiedztwa i Partnerstwa (ENPI);

h) studenci oraz studenci podyplomowi, którzy odbywają regularne podróże w celu podjęcia nauki lub udziału w szkoleniach, w tym w ramach programów wymiany;

i) przedstawiciele wspólnot wyznaniowych;

j) przedstawiciele wolnych zawodów biorący udział w międzynarodowych wystawach, konferencjach, sympozjach, seminariach lub innych podobnych imprezach odbywających się na terytorium państw członkowskich;

k) osoby zmuszone do odbywania regularnych podróży z powodów zdrowotnych i niezbędne osoby towarzyszące.

Na zasadzie odstępstwa od akapitu pierwszego, jeżeli konieczność lub zamiar częstego lub regularnego odbywania podróży są wyraźnie ograniczone do krótszego okresu, okres ważności wizy wielokrotnego wjazdu będzie ograniczony do tego okresu."

W pierwotnej wersji Umowy wyrażenie „o okresie ważności do jednego roku" pozostawiało konsulatom swobodę przy podejmowaniu decyzji w sprawie okresu ważności wizy, określając wyłącznie maksymalny okres ważności. W Umowie zmieniającej swoboda ta zniknęła wraz z wprowadzeniem nowego sformułowania „o jednorocznym okresie ważności", na podstawie którego, jeżeli wnioskodawca spełnia wszystkie wymogi art. 5 ust. 2 Umowy „Misje dyplomatyczne oraz służby konsularne państw członkowskich wydają wizy wielokrotnego wjazdu o jednorocznym okresie ważności". Należy zauważyć, że wizy wielokrotnego wjazdu ważne przez okres jednego roku wydaje się osobom należącym do wyżej wymienionych kategorii, jeżeli w poprzednim roku (12 miesięcy) osoba ubiegająca się o wizę uzyskała co najmniej jedną wizę Schengen, z której skorzystała zgodnie z przepisami dotyczącymi wjazdu do danego kraju (-ów) i pobytu w nim (nich)(na przykład osoba ta nie przekroczyła okresu dozwolonego pobytu) oraz jeżeli istnieją powody ubiegania się o wizę wielokrotnego wjazdu. Wiza Schengen otrzymana w poprzednim roku może być wydana przez państwo Schengen inne niż to, w którym wnioskodawca ubiega się o nową wizę. W przypadkach gdy wydanie wizy o jednorocznym okresie ważności nie jest uzasadnione (na przykład jeżeli okres trwania programu wymiany jest krótszy niż jeden rok lub nie występuje konieczność częstego lub regularnego podróżowania przez cały rok) okres ważności wizy będzie krótszy niż jeden rok, pod warunkiem że inne wymogi w odniesieniu do wydania wizy zostały spełnione.

Art. 5 ust.3 i 4 Umowy stwierdza, że:

„3. Misje dyplomatyczne oraz urzędy konsularne państw członkowskich wydają wizy wielokrotnego wjazdu o okresie ważności co najmniej dwóch lat i co najwyżej pięciu lat osobom wymienionym w ust. 2 niniejszego artykułu, pod warunkiem że w poprzednich dwóch latach takie osoby korzystały z jednorocznych wiz wielokrotnego wjazdu zgodnie z przepisami odwiedzanego państwa członkowskiego dotyczącymi wjazdu i pobytu, chyba że konieczność lub zamiar częstego lub regularnego odbywania podróży są wyraźnie ograniczone do krótszego okresu, w którym to przypadku okres ważności wizy wielokrotnego wjazdu ogranicza się do tego okresu.

4. Całkowity czas pobytu osób, o których mowa w ust. 1–3 niniejszego artykułu, na terytorium państw członkowskich nie może przekraczać 90 dni na każde 180 dni.".

Wizy wielokrotnego wjazdu o okresie ważności co najmniej dwóch lat i co najwyżej pięciu lat wydaje się osobom należącym do kategorii, o których mowa w art. 5 ust. 2 Umowy, pod warunkiem że w poprzednich dwóch latach takie osoby korzystały z jednorocznych wiz wielokrotnego wjazdu zgodnie z przepisami dotyczącymi wjazdu i pobytu na terytorium odwiedzanego (-ych) państwa (państw) oraz, że konieczność częstego lub regularnego odbywania podróży nie jest wyraźnie ograniczona do krótszego okresu. Należy zauważyć, że wiza o okresie ważności od dwóch do pięciu lat wydawana jest wyłącznie w przypadku, gdy osobie ubiegającej się o wizę w ciągu dwóch poprzednich lat wydano dwie wizy o ważności jednego roku, i osoba ta korzystała z tych wiz zgodnie z przepisami dotyczącymi wjazdu i pobytu na terytorium odwiedzanego (-ych) państwa (państw). Misje dyplomatyczne oraz urzędy konsularne państw członkowskich podejmują decyzję, na podstawie oceny każdego wniosku wizowego, dotyczącą okresu ważności wiz – tj. od dwóch do pięciu lat.

W odniesieniu do definicji kryteriów określonych w art. 5 ust. 2 Umowy: „pod warunkiem że […] wniosek o wizę wielokrotnego wjazdu jest uzasadniony" oraz art. 5 ust. 3 Umowy: „pod warunkiem że […] nadal aktualne są powody ubiegania się o wizę wielokrotnego wjazdu" stosuje się kryteria określone w art. 24 ust. 2 lit. a) kodeksu wizowego w odniesieniu do wydawania tego rodzaju wiz, tzn. że osoba ubiegająca się o wizę jest zmuszona do częstego i regularnego podróżowania do jednego lub kilku państw członkowskich, na przykład w celach służbowych.

Nie ma obowiązku wydawania wizy wielokrotnego wjazdu, jeżeli wnioskodawca nie skorzystał z poprzedniej wizy. Niemniej jednak taka wiza może zostać wydana w przypadku gdy niewykorzystanie wcześniejszej wizy jest spowodowane okolicznościami niezależnymi od woli wnioskodawcy; na przykład długotrwałą nieobecnością w pracy kierowcy samochodu ciężarowego z powodu choroby.

Por pkt II.2.2.1. dotyczący dokumentów uzasadniających cel podróży w odniesieniu do wydawania wiz wielokrotnego wjazdu osobom należącym do kategorii, o których mowa w art. 5 Umowy.

2.2.3. *Posiadacze paszportów dyplomatycznych i służbowych.*

Art. 10 Umowy stanowi:

„1. Obywatele Ukrainy będący w posiadaniu ważnego paszportu dyplomatycznego mogą wjechać na terytorium państw członkowskich, opuścić to terytorium lub przejechać przez nie bez wizy.

2. Obywatele Ukrainy będący w posiadaniu ważnego służbowego paszportu biometrycznego mogą wjechać na terytorium państw członkowskich, opuścić to terytorium lub przejechać przez nie bez wizy.

3. Osoby, o których mowa w ust. 1 i 2 niniejszego artykułu, mogą pozostać na terytorium państw członkowskich przez okres nieprzekraczający 90 dni w okresie 180 dni."

Istniejące umowy dwustronne lub ustalenia przewidujące zwolnienie z obowiązku wizowego dla posiadaczy nie biometrycznych paszportów służbowych nadal mają zastosowanie, chyba że zostaną wypowiedziane lub zawieszone (zob. 1.6).

Delegowanie dyplomatów do państw członkowskich nie zostało uregulowane w przedmiotowej umowie. Zastosowanie ma zwyczajowa procedura akredytacji.

III. STATYSTYKA

Aby umożliwić Wspólnemu Komitetowi skuteczne kontrolowanie jej wykonania, misje dyplomatyczne i urzędy konsularne państw członkowskich muszą przedkładać Komisji co sześć miesięcy dane statystyczne, w podziale na poszczególne miesiące, i dotyczące w szczególności, tam gdzie to możliwe:

— rodzaju wiz wydawanych osobom należącym do różnych kategorii objętych Umową;

— liczby decyzji odmownych w sprawie wydania wizy osobom należącym do różnych kategorii objętych Umową;

— odsetka wnioskodawców zaproszonych na rozmowy w podziale na kategorie osób;

— wiz wielokrotnego wjazdu o pięcioletnim okresie ważności wydanych obywatelom Ukrainy (w podziale na państwa).

— odsetka wiz wydawanych bezpłatnie w podziale na poszczególne kategorie osób objęte Umową.

DECYZJA RADY (WPZiB) 2015/439

z dnia 16 marca 2015 r.

przedłużająca mandat Specjalnego Przedstawiciela Unii Europejskiej w regionie Sahelu

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 33 i art. 31 ust. 2,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 18 marca 2013 r. Rada przyjęła decyzję 2013/133/WPZiB ([1]) w sprawie mianowania Michela Dominique'a REVEYRANDA – DE MENTHONA Specjalnym Przedstawicielem Unii Europejskiej (SPUE) w regionie Sahelu. Mandat SPUE został przedłużony decyzją Rady 2014/130/WPZiB ([2]) i wygasa w dniu 28 lutego 2015 r.

(2) Mandat SPUE należy przedłużyć na okres kolejnych ośmiu miesięcy.

(3) SPUE będzie wykonywał swój mandat w sytuacji, która może ulec pogorszeniu i mogłaby utrudnić osiągnięcie celów działań zewnętrznych Unii określonych w art. 21 Traktatu,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Specjalny Przedstawiciel Unii Europejskiej

1. Mandat Michela Dominique'a REVEYRANDA – DE MENTHONA na stanowisku SPUE w regionie Sahelu zostaje przedłużony do dnia 31 października 2015 r. Mandat SPUE może zostać skrócony, jeżeli Rada podejmie taką decyzję na wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (WP).

2. Do celów mandatu SPUE region Sahelu jest zdefiniowany jako obszar, na który główny nacisk położono w strategii UE na rzecz bezpieczeństwa i rozwoju w regionie Sahelu („Strategia"), to jest Burkina Faso, Czad, Mali, Mauretanię i Niger. W przypadku kwestii mających skutki dla szerzej rozumianego regionu SPUE współdziała – w stosownych przypadkach – z innymi państwami oraz podmiotami regionalnymi lub międzynarodowymi spoza regionu Sahelu, a także Afryki Zachodniej i regionu Zatoki Gwinejskiej.

3. W związku z potrzebą zastosowania podejścia regionalnego do wzajemnie powiązanych wyzwań dotyczących tego regionu, SPUE w regionie Sahelu prowadzi działania ściśle konsultując się z innymi odpowiednimi SPUE, w tym SPUE w południowym regionie Morza Śródziemnego, SPUE ds. Praw Człowieka oraz SPUE przy Unii Afrykańskiej.

Artykuł 2

Cele polityki

1. Mandat SPUE opiera się na celach polityki Unii w odniesieniu do regionu Sahelu i ma służyć aktywnemu wspieraniu regionalnych i międzynarodowych wysiłków na rzecz osiągnięcia trwałego pokoju, bezpieczeństwa i rozwoju w regionie. Celem SPUE jest ponadto poprawa jakości, intensywności i wpływu wieloaspektowego zaangażowania Unii w regionie Sahelu.

2. SPUE przyczynia się do rozwijania i wdrażania podejścia Unii obejmującego wszystkie aspekty działań Unii, w szczególności w dziedzinie polityki, bezpieczeństwa i rozwoju, w tym również Strategii, oraz do koordynowania wszystkich odpowiednich instrumentów działań Unii.

3. Początkowo kwestią priorytetową jest Mali i jego długotrwała stabilizacja oraz regionalne wymiary konfliktu w tym państwie.

([1]) Decyzja Rady 2013/133/WPZiB z dnia 18 marca 2013 r. w sprawie mianowania Specjalnego Przedstawiciela Unii Europejskiej w regionie Sahelu (Dz.U. L 75 z 19.3.2013, s. 29).

([2]) Decyzja Rady 2014/130/WPZiB z dnia 10 marca 2014 r. przedłużająca mandat Specjalnego Przedstawiciela Unii Europejskiej w regionie Sahelu (Dz.U. L 71 z 12.3.2014, s. 14).

4. W odniesieniu do Mali cele polityki Unii to propagowanie, poprzez skoordynowane i efektywne wykorzystywanie wszystkich dostępnych jej instrumentów, powrotu Mali i jego ludności na drogę pokoju, pojednania, bezpieczeństwa i rozwoju. Szczególną uwagę należy także poświęcić Burkina Faso i Nigrowi, w szczególności w związku ze zbliżającymi się wyborami w tych państwach.

Artykuł 3

Mandat

1. Dla osiągnięcia celów polityki Unii w odniesieniu do regionu Sahelu mandat SPUE obejmuje:

a) aktywne przyczynianie się do wdrażania, koordynacji i dalszego rozwijania kompleksowego podejścia Unii do kryzysu w regionie, na podstawie jej Strategii, w celu zwiększenia ogólnej spójności i skuteczności działań Unii w regionie Sahelu, a w szczególności w Mali;

b) współpracę z wszystkimi odpowiednimi zainteresowanymi podmiotami w regionie, rządami, władzami regionalnymi, organizacjami regionalnymi i międzynarodowymi, społeczeństwem obywatelskim i diasporą, z myślą o realizacji celów Unii i przyczyniania się do lepszego rozumienia roli Unii w regionie Sahelu;

c) reprezentowanie Unii na odpowiednich forach regionalnych i międzynarodowych, w tym w grupie ds. wsparcia i monitorowania sytuacji w Mali, oraz zapewnianie widoczności pomocy Unii w zarządzaniu kryzysowym i zapobieganiu konfliktom, w tym misji wojskowej Unii Europejskiej mającej na celu przyczynienie się do szkolenia malijskich sił zbrojnych (EUTM Mali) oraz misji Unii Europejskiej w dziedzinie WPBiO w Nigrze (EUCAP SAHEL Niger);

d) utrzymywanie ścisłej współpracy z Organizacją Narodów Zjednoczonych (ONZ), w szczególności ze Specjalnym Przedstawicielem Sekretarza Generalnego ONZ ds. Afryki Zachodniej i Specjalnym Przedstawicielem Sekretarza Generalnego ONZ ds. Mali, Unią Afrykańską (UA), w szczególności Wysokim Przedstawicielem UA ds. Mali i Sahelu, Wspólnotą Gospodarczą Państw Afryki Zachodniej (ECOWAS) oraz innymi istotnymi zainteresowanymi podmiotami krajowymi, regionalnymi i międzynarodowymi, w tym ze specjalnymi wysłannikami ds. regionu Sahelu, a także odpowiednimi podmiotami w obszarze Maghrebu;

e) skrupulatne monitorowanie regionalnego i ponadgranicznego wymiaru kryzysu, w tym terroryzmu, przestępczości zorganizowanej, przemytu broni, handlu ludźmi, handlu narkotykami, przepływów migracyjnych i uchodźców oraz związanych z nimi przepływów finansowych, a także – w ścisłej współpracy z Koordynatorem UE ds. Zwalczania Terroryzmu – przyczynianie się do dalszej realizacji strategii UE w dziedzinie walki z terroryzmem;

f) utrzymywanie regularnych kontaktów politycznych wysokiego szczebla z państwami w regionie dotkniętymi terroryzmem i przestępczością międzynarodową w celu zapewnienia spójnego i wszechstronnego podejścia i odgrywania przez Unię kluczowej roli w międzynarodowych wysiłkach na rzecz zwalczania terroryzmu i międzynarodowej przestępczości. Obejmuje to aktywne wspieranie przez Unię regionalnego budowania zdolności w zakresie bezpieczeństwa i zapewnianie odpowiednich działań służących zwalczaniu źródeł terroryzmu i przestępczości międzynarodowej w regionie Sahelu;

g) dokładne śledzenie konsekwencji politycznych i w zakresie bezpieczeństwa wynikających z kryzysu humanitarnego w regionie;

h) w odniesieniu do Mali – przyczynianie się do regionalnych i międzynarodowych działań z myślą o ułatwieniu zakończenia kryzysu w Mali, w szczególności całkowitego przywrócenia normalnych warunków konstytucyjnych i rządów na całym terytorium i rzeczywistego pluralistycznego dialogu ogólnonarodowego prowadzącego do zrównoważonego porozumienia politycznego;

i) propagowanie tworzenia instytucji, reformy sektora bezpieczeństwa i długoterminowego procesu pokojowego oraz pojednania w Mali;

j) przyczynianie się do realizacji w regionie, we współpracy ze SPUE ds. Praw Człowieka, polityk Unii w dziedzinie praw człowieka – w tym wytycznych UE w sprawie praw człowieka, w szczególności wytycznych UE w sprawie dzieci w konfliktach zbrojnych, a także w sprawie aktów przemocy wobec kobiet i zwalczania wszelkich form dyskryminacji kobiet – oraz unijnej polityki na rzecz kobiet, pokoju i bezpieczeństwa, w tym poprzez monitorowanie rozwoju sytuacji i przygotowywanie dotyczących jej sprawozdań, a także formułowanie stosownych zaleceń; oraz utrzymywanie regularnych kontaktów z właściwymi organami w Mali i regionie, biurem prokuratora Międzynarodowego Trybunału Karnego, biurem Wysokiego Komisarza ds. Praw Człowieka oraz obrońcami praw człowieka i obserwatorami w regionie;

k) monitorowanie przestrzegania właściwych rezolucji Rady Bezpieczeństwa ONZ (RB ONZ) – i składanie stosownych sprawozdań – w szczególności w odniesieniu do rezolucji RB ONZ nr 2056 (2012), 2071 (2012), 2085 (2012) i 2100 (2013).

2. W celu sprawowania swojego mandatu SPUE między innymi:

a) doradza i składa sprawozdania w zakresie formułowania stanowiska Unii na forach regionalnych i międzynarodowych – w zależności od potrzeby, aby aktywnie propagować i wzmacniać wszechstronne podejście UE do kryzysu w regionie Sahelu;

b) utrzymuje ogólny ogląd wszystkich działań Unii i współpracuje ściśle z odpowiednimi delegaturami Unii.

Artykuł 4

Wykonywanie mandatu

1. SPUE jest odpowiedzialny za wykonywanie mandatu działając pod zwierzchnictwem WP.

2. Komitet Polityczny i Bezpieczeństwa (KPiB) utrzymuje uprzywilejowane stosunki ze SPUE i jest podstawowym punktem kontaktowym SPUE z Radą. KPiB ukierunkowuje pod względem strategicznym i politycznym działania wykonywane przez SPUE w ramach mandatu, bez uszczerbku dla uprawnień WP.

3. SPUE ściśle koordynuje swoje działania z działaniami Europejskiej Służby Działań Zewnętrznych (ESDZ) i jej odpowiednimi departamentami, w szczególności koordynatorem w regionie Sahelu.

Artykuł 5

Finansowanie

1. Finansowa kwota odniesienia przewidziana na pokrycie wydatków związanych z mandatem SPUE w okresie od dnia 1 marca 2015 r. do dnia 31 października 2015 r. wynosi 900 000 EUR.

2. Wydatkami zarządza się zgodnie z procedurami i przepisami mającymi zastosowanie do budżetu ogólnego Unii.

3. Zarządzanie wydatkami podlega umowie między SPUE a Komisją. SPUE odpowiada przed Komisją za wszystkie wydatki.

Artykuł 6

Powołanie i skład zespołu

1. W granicach swojego mandatu i odpowiednich dostępnych środków finansowych SPUE odpowiada za powołanie swojego zespołu. Zespół dysponuje wiedzą fachową na temat konkretnych kwestii politycznych i dotyczących bezpieczeństwa związanych z mandatem. SPUE informuje niezwłocznie Radę i Komisję o składzie swojego zespołu.

2. Państwa członkowskie, instytucje Unii i ESDZ mogą zaproponować oddelegowanie personelu do pracy ze SPUE. Wynagrodzenie takiego personelu oddelegowanego do obsługi SPUE jest pokrywane przez dane państwo członkowskie, daną instytucję Unii lub przez ESDZ. Eksperci oddelegowani przez państwa członkowskie do instytucji Unii lub do ESDZ również mogą być oddelegowani do SPUE. Zatrudniani na podstawie umów członkowie personelu międzynarodowego mają obywatelstwo państwa członkowskiego.

3. Cały oddelegowany personel nadal podlega administracyjnie wysyłającemu państwu członkowskiemu, wysyłającej instytucji Unii lub ESDZ; personel ten wypełnia obowiązki i podejmuje działania w interesie mandatu SPUE.

4. Personel SPUE ulokowany jest w tym samym miejscu co właściwe departamenty ESDZ lub delegatury Unii, aby zapewnić spójność i zgodność ich działań.

Artykuł 7

Przywileje i immunitety SPUE i jego personelu

Przywileje, immunitety i dalsze gwarancje niezbędne do wykonania i sprawnego działania misji SPUE oraz członków jego personelu ustala się odpowiednio z państwami przyjmującymi. Państwa członkowskie i ESDZ zapewniają wszelkie niezbędne w tym celu wsparcie.

Artykuł 8

Bezpieczeństwo informacji niejawnych UE

SPUE i członkowie jego zespołu przestrzegają zasad i minimalnych norm bezpieczeństwa ustanowionych decyzją Rady 2013/488/UE ([1]).

([1]) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).

Artykuł 9

Dostęp do informacji i wsparcie logistyczne

1. Państwa członkowskie, Komisja, ESDZ oraz Sekretariat Generalny Rady zapewniają SPUE dostęp do wszelkich stosownych informacji.

2. Delegatury Unii lub, w stosownych przypadkach, państwa członkowskie zapewniają wsparcie logistyczne w regionie.

Artykuł 10

Bezpieczeństwo

Zgodnie z polityką Unii dotyczącą bezpieczeństwa personelu rozmieszczonego poza terytorium Unii w ramach zadań operacyjnych zgodnie z tytułem V Traktatu SPUE przyjmuje wszelkie uzasadnione, możliwe do realizacji środki zgodne z jego mandatem oraz odpowiadające stanowi bezpieczeństwa na obszarze geograficznym, za który jest odpowiedzialny, służące zapewnieniu bezpieczeństwa całemu personelowi bezpośrednio mu podlegającemu, w szczególności:

a) sporządza plan bezpieczeństwa oparty na wytycznych ESDZ, obejmujący specyficzne fizyczne, organizacyjne i proceduralne środki bezpieczeństwa, regulujący zarządzanie bezpiecznym przemieszczaniem się personelu do tego obszaru geograficznego i w jego obrębie, jak również reagowanie na zdarzenia związane z naruszaniem bezpieczeństwa, a także plan awaryjny i ewakuacyjny misji;

b) zapewnia objęcie wszystkich członków personelu rozmieszczonych poza terytorium Unii ubezpieczeniem od wysokiego ryzyka odpowiednio do warunków panujących na tym obszarze geograficznym;

c) zapewnia, aby wszyscy członkowie jego zespołu, którzy mają być rozmieszczeni poza terytorium Unii, w tym zatrudniony na podstawie umów personel miejscowy, odbyli przed przyjazdem na obszar misji lub niezwłocznie po przyjeździe odpowiednie szkolenie w zakresie bezpieczeństwa, na podstawie wskaźników ryzyka określonych dla tego obszaru geograficznego;

d) zapewnia wdrożenie wszelkich uzgodnionych zaleceń wydanych po dokonaniu regularnych ocen bezpieczeństwa oraz – w ramach sprawozdania o postępach oraz sprawozdania z wykonania mandatu – przedstawia Radzie, WP i Komisji pisemne sprawozdania dotyczące wdrażania tych zaleceń oraz innych kwestii związanych z bezpieczeństwem.

Artykuł 11

Składanie sprawozdań

1. SPUE regularnie składa WP i KPiB sprawozdania. W razie potrzeby SPUE składa również sprawozdania grupom roboczym Rady. Regularne sprawozdania są rozprowadzane poprzez sieć COREU. SPUE może przedstawiać sprawozdania Radzie do Spraw Zagranicznych. Zgodnie z art. 36 Traktatu SPUE może uczestniczyć w przekazywaniu informacji Parlamentowi Europejskiemu.

2. SPUE składa sprawozdania dotyczące najlepszego sposobu realizacji inicjatyw Unii, takich jak jej wkład w reformy, z uwzględnieniem politycznych aspektów odnośnych projektów rozwojowych Unii, w koordynacji z delegaturami Unii w regionie.

Artykuł 12

Koordynacja z innymi podmiotami unijnymi

1. SPUE w ramach Strategii przyczynia się do jedności, spójności i efektywności unijnych działań politycznych i dyplomatycznych oraz pomaga zapewnić spójne wykorzystanie wszystkich instrumentów Unii i działań państw członkowskich, aby osiągnąć cele polityki Unii.

2. SPUE koordynuje swoje działania z działaniami delegatur Unii i Komisji, jak również z działaniami innych SPUE działających w regionie. SPUE regularnie przekazuje informacje działającym w regionie misjom państw członkowskich i delegaturom Unii.

3. SPUE utrzymuje ścisłą współpracę w terenie z szefami delegatur Unii i z szefami misji państw członkowskich. SPUE, w ścisłej współpracy z właściwymi delegaturami Unii, zapewnia szefom misji EUCAP Sahel Niger i EUCAP Sahel Mali oraz dowódcy misji EUTM Mali wytyczne w zakresie sytuacji politycznej na miejscu. W razie potrzeby SPUE, dowódca misji EUTM Mali i cywilny dowódca operacji EUCAP Sahel Niger i EUCAP Sahel Mali zasięgają nawzajem swojej opinii.

Artykuł 13

Przegląd

Wdrażanie niniejszej decyzji i jej spójność z innymi działaniami Unii w regionie są przedmiotem regularnych przeglądów. Przed końcem sierpnia 2015 r. SPUE przedstawi Radzie, WP i Komisji kompleksowe sprawozdanie z wykonania mandatu.

Artykuł 14

Wejście w życie

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Niniejszą decyzję stosuje się od dnia 1 marca 2015 r.

Sporządzono w Brukseli dnia 16 marca 2015 r.

W imieniu Rady
F. MOGHERINI
Przewodniczący

DECYZJA RADY (WPZiB) 2015/440

z dnia 16 marca 2015 r.

przedłużająca mandat Specjalnego Przedstawiciela Unii Europejskiej w Rogu Afryki

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 33 i art. 31 ust. 2,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 8 grudnia 2011 r. Rada przyjęła decyzję 2011/819/WPZiB [1] w sprawie mianowania Alexandra RONDOSA Specjalnym Przedstawicielem Unii Europejskiej (SPUE) w Rogu Afryki. Mandat SPUE wygaśnie w dniu 28 lutego 2015 r.

(2) Mandat SPUE należy przedłużyć do dnia 31 października 2015 r.

(3) SPUE będzie wykonywał mandat w sytuacji, która może ulec pogorszeniu i mogłaby utrudnić osiągnięcie celów działań zewnętrznych Unii określonych w art. 21 Traktatu,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Specjalny Przedstawiciel Unii Europejskiej

Mandat Alexandra Rondosa jako SPUE w Rogu Afryki zostaje przedłużony do dnia 31 października 2015 r. Rada może zadecydować, że mandat SPUE zostanie zakończony wcześniej, w oparciu o ocenę dokonaną przez Komitet Polityczny i Bezpieczeństwa (KPiB) oraz wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (WP).

Na potrzeby mandatu SPUE Róg Afryki definiuje się jako region obejmujący Republikę Dżibuti, Państwo Erytreę, Federalną Demokratyczną Republikę Etiopii, Republikę Kenii, Federalną Republikę Somalii, Republikę Sudanu, Republikę Sudanu Południowego oraz Republikę Ugandy. W kwestiach o szerszym zasięgu regionalnym SPUE współpracuje w stosownych przypadkach z państwami i podmiotami regionalnymi spoza Rogu Afryki.

Artykuł 2

Cele polityki

1. Mandat SPUE opiera się na celach polityki Unii wobec Rogu Afryki określonych w ramach strategicznych przyjętych w dniu 14 listopada 2011 r. i w odnośnych konkluzjach Rady, które to cele zakładają aktywny wkład w regionalne i międzynarodowe starania na rzecz zapewnienia pokojowego współistnienia i trwałego pokoju, bezpieczeństwa i rozwoju wewnątrz państw regionu i w stosunkach między nimi. Celem SPUE jest ponadto poprawa jakości, intensywności, efektów i wyeksponowania wielopłaszczyznowego zaangażowania Unii w Rogu Afryki.

2. Do celów polityki należą między innymi:

a) ciągła stabilizacja sytuacji w Somalii, w szczególności w kontekście regionalnym;

b) pokojowe współistnienie Sudanu i Sudanu Południowego jako dwóch stabilnych i bogatych państw posiadających solidne i odpowiedzialne struktury polityczne;

c) rozwiązanie aktualnych konfliktów oraz zapobieganie potencjalnym konfliktom między państwami regionu lub wewnątrz tych państw;

d) wspieranie współpracy regionalnej w zakresie polityki, bezpieczeństwa i gospodarki.

[1] Decyzja Rady 2011/819/WPZiB z dnia 8 grudnia 2011 r. w sprawie mianowania Specjalnego Przedstawiciela Unii Europejskiej w Rogu Afryki (Dz.U. L 327 z 9.12.2011, s. 62).

Artykuł 3

Mandat

1. Aby umożliwić osiągnięcie celów polityki Unii wobec Rogu Afryki, mandat SPUE obejmuje:

a) współpracę ze wszystkimi właściwymi podmiotami w regionie, rządami, władzami regionalnymi, organizacjami międzynarodowymi i regionalnymi, społeczeństwem obywatelskim oraz diasporami, służącą czynieniu postępów w realizacji celów Unii i przyczyniającą się do lepszego zrozumienia roli Unii w tym regionie;

b) reprezentowanie Unii, w stosownych przypadkach, na właściwych forach międzynarodowych i czuwanie nad tym, by udzielane przez Unię wsparcie w dziedzinie zarządzania kryzysowego oraz rozwiązywania konfliktów i zapobiegania im było odpowiednio wyeksponowane;

c) zachęcanie do skutecznej współpracy w zakresie polityki i bezpieczeństwa oraz do integracji gospodarczej, na szczeblu regionalnym, oraz wspieranie takiej współpracy i integracji, poprzez partnerstwo Unii z Unią Afrykańską (UA) i organizacjami regionalnymi, w szczególności Międzyrządowym Organem ds. Rozwoju (IGAD);

d) śledzenie wydarzeń politycznych w regionie i wnoszenie wkładu w formułowanie polityki Unii wobec regionu, w tym w odniesieniu do Somalii, Sudanu, Sudanu Południowego, kwestii granicy między Etiopią a Erytreą i realizacji porozumienia algierskiego, inicjatywy dorzecza Nilu, a także w odniesieniu do innych problemów w regionie, które mają wpływ na jego bezpieczeństwo, stabilność i dobrobyt;

e) w odniesieniu do Somalii oraz w ścisłej koordynacji ze specjalnym wysłannikiem UE w Somalii i odnośnymi partnerami regionalnymi i międzynarodowymi, w tym specjalnym przedstawicielem sekretarza generalnego ONZ w Somalii i UA – aktywne wnoszenie wkładu w działania i inicjatywy prowadzące do dalszej stabilizacji i kolejnych rozwiązań na okres przejściowy w Somalii, z naciskiem na propagowanie skoordynowanego i spójnego międzynarodowego podejścia do Somalii, budowanie stosunków dobrosąsiedzkich i wspieranie rozwoju somalijskiego sektora bezpieczeństwa, m.in. za pośrednictwem misji wojskowej Unii Europejskiej mającej na celu przyczynienie się do szkolenia somalijskich sił bezpieczeństwa (EUTM Somalia), dowodzonych przez Unię sił morskich (EUNAVFOR Atalanta), misji Unii Europejskiej dotyczącej budowania regionalnych zdolności morskich w Rogu Afryki (EUCAP Nestor) oraz za pośrednictwem stałego unijnego wsparcia Misji Unii Afrykańskiej w Somalii (AMISOM) – w ścisłej współpracy z państwami członkowskimi;

f) w odniesieniu do Sudanu i Sudanu Południowego oraz w ścisłej współpracy z właściwymi szefami delegatur Unii – wnoszenie wkładu w spójność i skuteczność polityki Unii wobec Sudanu i Sudanu Południowego oraz wspieranie pokojowego współistnienia tych państw, w szczególności przez realizację porozumień z Addis Abeby i rozwiązanie nierozstrzygniętych kwestii wynikających z wygaśnięcia całościowego porozumienia pokojowego, w tym: kwestii Abyei, politycznego rozwiązania trwających konfliktów, zwłaszcza w Darfurze, Kordofanie Południowym i prowincji Nilu Błękitnego, rozwoju instytucjonalnego w Sudanie Południowym i pojednania narodowego. W tym względzie SPUE wnosi wkład w spójne międzynarodowe podejście, w ścisłej współpracy z UA, a w szczególności z panelem wykonawczym wysokiego szczebla z ramienia UA do spraw Sudanu (AUHIP), ONZ i innymi istotnymi podmiotami regionalnymi i międzynarodowymi;

g) dokładne obserwowanie wyzwań transgranicznych, przed którymi staje Róg Afryki, obejmujących terroryzm, radykalizację postaw, bezpieczeństwo morskie i piractwo, przestępczość zorganizowaną, przemyt broni, przepływ uchodźców i migrantów, oraz wszelkich konsekwencji kryzysów humanitarnych dla polityki i bezpieczeństwa;

h) propagowanie dostępu pomocy humanitarnej w całym regionie;

i) wnoszenie wkładu we wdrażanie decyzji Rady 2011/168/WPZiB [1] oraz unijnej polityki w dziedzinie praw człowieka (we współpracy ze SPUE ds. Praw Człowieka) w tym wytycznych UE w dziedzinie praw człowieka – w szczególności wytycznych UE w sprawie dzieci w konfliktach zbrojnych, a także wytycznych UE w sprawie aktów przemocy wobec kobiet i zwalczania wszelkich form dyskryminacji kobiet – oraz polityki Unii w odniesieniu do rezolucji Rady Bezpieczeństwa ONZ 1325 (2000), m.in. poprzez monitorowanie rozwoju sytuacji i opracowywanie sprawozdań na ten temat, a także formułowanie stosownych zaleceń.

2. W celu sprawowania mandatu SPUE między innymi:

a) doradza i składa sprawozdania w sprawie określania stanowisk Unii na forach międzynarodowych, w stosownych przypadkach, aby w sposób proaktywny wspierać wszechstronne podejście wobec Rogu Afryki w ramach polityki Unii;

b) obserwuje wszelkie działania Unii.

[1] Decyzja Rady 2011/168/WPZiB z dnia 21 marca 2011 r. w sprawie Międzynarodowego Trybunału Karnego, uchylająca wspólne stanowisko 2003/444/WPZiB (Dz.U. L 76 z 22.3.2011, s. 56).

Artykuł 4

Wykonywanie mandatu

1. SPUE jest odpowiedzialny za wykonywanie mandatu, działając pod zwierzchnictwem WP.

2. KPiB utrzymuje uprzywilejowane stosunki ze SPUE i jest podstawowym punktem kontaktowym SPUE z Radą. KPiB ukierunkowuje pod względem strategicznym i politycznym działania prowadzone przez SPUE w ramach jego mandatu, bez uszczerbku dla uprawnień WP.

3. SPUE działa w ścisłej koordynacji z Europejską Służbą Działań Zewnętrznych (ESDZ) i jej właściwymi działami, delegaturami Unii w regionie oraz z Komisją.

Artykuł 5

Finansowanie

1. Finansowa kwota odniesienia przewidziana na pokrycie wydatków związanych z mandatem SPUE w okresie od dnia 1 marca 2015 r. do dnia 31 października 2015 r. wynosi 1 770 000 EUR.

2. Wydatkami zarządza się zgodnie z procedurami i zasadami mającymi zastosowanie do budżetu ogólnego Unii.

3. Zarządzanie wydatkami podlega umowie między SPUE a Komisją. SPUE odpowiada przed Komisją za wszystkie wydatki.

Artykuł 6

Powołanie i skład zespołu

1. W granicach mandatu SPUE i udostępnionych na jego potrzeby środków finansowych SPUE odpowiada za powołanie zespołu. Zespół dysponuje wiedzą fachową na temat konkretnych kwestii politycznych oraz dotyczących bezpieczeństwa związanych z mandatem. SPUE niezwłocznie i regularnie informuje Radę i Komisję o składzie swojego zespołu.

2. Państwa członkowskie, instytucje Unii i ESDZ mogą zaproponować oddelegowanie personelu do pracy ze SPUE. Wynagrodzenie takiego oddelegowanego personelu jest pokrywane, odpowiednio, przez dane państwo członkowskie, daną instytucję Unii lub ESDZ. Eksperci oddelegowani przez państwa członkowskie do instytucji Unii lub do ESDZ również mogą być oddelegowani do SPUE. Zatrudniani na podstawie umów członkowie personelu międzynarodowego muszą mieć obywatelstwo jednego z państw członkowskich.

3. Cały oddelegowany personel nadal podlega administracyjnie wysyłającemu państwu członkowskiemu, wysyłającej instytucji Unii lub ESDZ; personel ten wypełnia swoje obowiązki i podejmuje działania w interesie mandatu SPUE.

4. Personel SPUE ulokowany jest w tym samym miejscu co właściwe działy ESDZ lub delegatury Unii, co ma przyczyniać się do spójności i zgodności ich działań.

Artykuł 7

Przywileje i immunitety SPUE oraz personelu SPUE

Przywileje, immunitety i inne gwarancje niezbędne do wykonania i sprawnego działania misji SPUE oraz personelu SPUE ustala się odpowiednio z państwami przyjmującymi. Państwa członkowskie i ESDZ zapewniają w tym celu wszelkie niezbędne wsparcie.

Artykuł 8

Bezpieczeństwo informacji niejawnych UE

SPUE i członkowie jego zespołu przestrzegają zasad i minimalnych norm bezpieczeństwa ustanowionych decyzją Rady 2013/488/UE ([1]).

([1]) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).

Artykuł 9

Dostęp do informacji i wsparcie logistyczne

1. Państwa członkowskie, Komisja, ESDZ oraz Sekretariat Generalny Rady zapewniają SPUE dostęp do wszelkich stosownych informacji.

2. Delegatury Unii w regionie i państwa członkowskie, w stosownych przypadkach, zapewniają wsparcie logistyczne w regionie.

Artykuł 10

Bezpieczeństwo

Stosownie do polityki Unii dotyczącej bezpieczeństwa personelu rozmieszczonego poza terytorium Unii w ramach zadań operacyjnych na mocy tytułu V Traktatu, SPUE podejmuje wszystkie uzasadnione, możliwe do realizacji środki zgodne ze swoim mandatem oraz odpowiadające stanowi bezpieczeństwa na obszarze geograficznym, za który jest on odpowiedzialny, służące zapewnieniu bezpieczeństwa całemu personelowi bezpośrednio podlegającemu SPUE, w szczególności:

a) sporządza plan bezpieczeństwa dostosowany do potrzeb misji, oparty na wytycznych ESDZ, obejmujący fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dostosowane do potrzeb misji, zarządzanie bezpiecznym przemieszczaniem się personelu na obszar misji i w jego obrębie oraz reagowanie na zdarzenia zagrażające bezpieczeństwu, a także przewidujący plan awaryjny i plan ewakuacji misji;

b) zapewnia objęcie wszystkich członków personelu rozmieszczonych poza terytorium Unii ubezpieczeniem od wysokiego ryzyka, odpowiednio do warunków panujących na obszarze misji;

c) zapewnia, aby wszyscy członkowie zespołu SPUE, którzy mają być rozmieszczeni poza terytorium Unii, w tym personel miejscowy zatrudniony na podstawie umów, odbyli przed przyjazdem na obszar misji lub niezwłocznie po przyjeździe odpowiednie szkolenie w zakresie bezpieczeństwa, na podstawie wskaźników ryzyka określonych przez ESDZ dla obszaru misji;

d) zapewnia wdrażanie wszystkich uzgodnionych zaleceń wydawanych w następstwie systematycznych ocen bezpieczeństwa oraz – w ramach sprawozdania z postępu prac oraz sprawozdania z wykonania mandatu – dostarcza Radzie, WP i Komisji pisemne sprawozdania dotyczące wdrażania tych zaleceń oraz dotyczące innych kwestii związanych z bezpieczeństwem.

Artykuł 11

Sprawozdawczość

1. SPUE regularnie składa WP oraz KPiB sprawozdania ustne i pisemne. W razie potrzeby SPUE składa również sprawozdania grupom roboczym Rady. Regularne sprawozdania są rozprowadzane poprzez sieć COREU. SPUE może przedstawiać sprawozdania Radzie do Spraw Zagranicznych. Zgodnie z art. 36 Traktatu SPUE może uczestniczyć w informowaniu Parlamentu Europejskiego.

2. SPUE składa sprawozdania dotyczące najlepszego sposobu realizacji inicjatyw Unii – takich jak jej wkład w reformy – z uwzględnieniem politycznych aspektów odnośnych unijnych projektów rozwojowych, w koordynacji z delegaturami Unii w regionie.

Artykuł 12

Koordynacja

1. SPUE przyczynia się do jedności, spójności i skuteczności działań Unii i pomaga w zapewnieniu spójnego wykorzystania wszystkich instrumentów Unii i działań państw członkowskich, aby osiągnąć cele polityki Unii. SPUE koordynuje swoje działania z działaniami delegatur Unii i Komisji. SPUE regularnie przekazuje informacje działającym w regionie misjom państw członkowskich i delegaturom Unii.

2. Utrzymywany jest ścisły kontakt w terenie z szefami delegatur Unii i szefami misji państw członkowskich. Dokładają oni wszelkich starań, aby wspierać SPUE w wykonywaniu mandatu. SPUE, w ścisłej koordynacji z właściwymi delegaturami Unii, udziela dowódcy sił EU NAVFOR Atalanta, dowódcy UE misji EUTM Somalia oraz szefowi misji EUCAP Nestor wskazówek dotyczących sytuacji politycznej na miejscu. SPUE, dowódcy operacji UE oraz cywilny dowódca operacji konsultują się ze sobą stosownie do potrzeb.

3. SPUE ściśle współpracuje z władzami zaangażowanych państw, z ONZ, UA, IGAD, innymi podmiotami krajowymi, regionalnymi i międzynarodowymi, a także ze społeczeństwem obywatelskim w regionie.

Artykuł 13

Przegląd

Wdrażanie niniejszej decyzji i jej spójność z innymi działaniami Unii w regionie są przedmiotem regularnego przeglądu. SPUE przedstawi Radzie, WP i Komisji kompleksowe sprawozdanie z wykonania mandatu przed dniem 31 sierpnia 2015 r.

Artykuł 14

Wejście w życie

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Niniejsza decyzja jest stosowana od dnia 1 marca 2015 r.

Sporządzono w Brukseli dnia 16 marca 2015 r.

W imieniu Rady
F. MOGHERINI
Przewodniczący

DECYZJA RADY (WPZiB) 2015/441

z dnia 16 marca 2015 r.

dotycząca zmiany oraz przedłużenia decyzji 2010/96/WPZiB w sprawie misji wojskowej Unii Europejskiej mającej na celu przyczynienie się do szkolenia somalijskich sił bezpieczeństwa

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 42 ust. 4 i art. 43 ust. 2,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 15 lutego 2010 r. Rada przyjęła decyzję 2010/96/WPZiB ([1]). Mandat misji wojskowej UE zostanie zakończony w dniu 31 marca 2015 r.

(2) Brukselska konferencja w sprawie Somalii, zorganizowana w dniu 16 września 2013 r., zapewniła podstawy porozumienia w sprawie Somalii oraz zainicjowała mechanizm służący koordynacji i zapewnieniu odpowiedzialności Somalii za pośrednictwem grupy zadaniowej ds. nowego ładu dla Somalii („Somalia New Deal task force").

(3) W dniu 18 września 2014 r. w Londynie podczas międzynarodowego posiedzenia, którego współgospodarzami były Zjednoczone Królestwo i Somalia, rząd federalny nakreślił zaproponowaną przez ministerstwo obrony ścieżkę rozwoju somalijskiej armii krajowej aż do roku 2019 r., a także wskazał, co jest jej najpilniej potrzebne.

(4) Zgodnie z ustaleniami przeglądu strategicznego z października 2014 r., mandat misji wojskowej UE powinien zostać przedłużony do dnia 31 grudnia 2016 r.

(5) Zgodnie z art. 5 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w opracowywaniu oraz wprowadzaniu w życie decyzji i działań Unii, które mają wpływ na kwestie polityczno-obronne. Dania nie uczestniczy we wprowadzaniu w życie niniejszej decyzji ani nie współfinansuje niniejszej misji.

(6) Mandat misji wojskowej UE powinien zostać przedłużony ze zmienionym mandatem,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W decyzji 2010/96/WPZiB wprowadza się następujące zmiany:

1) art. 1 ust. 2 otrzymuje brzmienie:

„2. Z myślą o osiągnięciu celów określonych w ust. 1 misja wojskowa UE jest rozmieszczona w Somalii, aby dostarczać wskazówek strategicznych w zakresie rozwoju instytucjonalnego w sektorze obronnym, a także świadczyć bezpośrednie wsparcie somalijskiej armii krajowej w postaci szkolenia, doradztwa i pomocy mentorskiej. Misja wojskowa UE jest również gotowa świadczyć wsparcie innym podmiotom unijnym – w granicach swoich środków i zdolności – w realizacji ich odnośnych mandatów w dziedzinie bezpieczeństwa i obrony w Somalii.";

2) art. 3 otrzymuje brzmienie:

„*Artykuł 3*

Wyznaczenie dowództwa misji

1. Dowództwo misji znajduje się w Somalii, w Międzynarodowym Porcie Lotniczym Mogadiszu w Mogadiszu. Pełni funkcje zarówno dowództwa operacji, jak i dowództwa sił.

2. Do dowództwa misji zalicza się biuro łącznikowe i ds. wsparcia w Nairobi oraz komórkę wsparcia w Brukseli.";

([1]) Decyzja Rady 2010/96/WPZiB z dnia 15 lutego 2010 r. w sprawie misji wojskowej Unii Europejskiej mającej na celu przyczynienie się do szkolenia somalijskich sił bezpieczeństwa (Dz.U. L 44 z 19.2.2010, s. 16).

3) art. 7 ust. 4 otrzymuje brzmienie:

„4. Misja wojskowa UE – w granicach swoich środków i zdolności – prowadzi działania w ścisłej współpracy z innymi podmiotami międzynarodowymi w regionie, w szczególności z Organizacją Narodów Zjednoczonych i AMISOM, w myśl uzgodnionych wymogów federalnego rządu Somalii.";

4) w art. 10 dodaje się ustęp w brzmieniu:

„5. Finansowa kwota odniesienia dla wspólnych kosztów misji wojskowej UE na okres od dnia 1 kwietnia 2015 r. do dnia 31 grudnia 2016 r. wynosi 17 507 399 EUR. Odsetek tej kwoty odniesienia, o którym mowa w art. 25 ust. 1 decyzji Athena, wynosi 30 %, a odsetek dla zobowiązania, o którym mowa w art. 32 ust. 3 decyzji Athena, wynosi 90 %.";

5) dodaje się artykuł w brzmieniu:

„Artykuł 10b

Komórka ds. projektów

1. W skład misji wojskowej UE wchodzi komórka ds. projektów określająca i realizująca projekty, które mają być finansowane przez państwa członkowskie lub państwa trzecie i które są zgodne z celami misji i przyczyniają się do realizacji jej mandatu.

2. Z zastrzeżeniem ust. 3 dowódca misji UE jest upoważniony do korzystania z wkładów finansowych państw członkowskich lub państw trzecich w celu realizacji określonych projektów, które w spójny sposób uzupełniają inne działania misji wojskowej UE. W takim przypadku dowódca misji UE zawiera uzgodnienie z tymi państwami, obejmujące w szczególności konkretne zasady postępowania z wszelkiego rodzaju skargami stron trzecich w zakresie szkód zaistniałych z powodu działań lub zaniechania działań ze strony dowódcy misji UE w związku z korzystaniem ze środków finansowych udostępnionych przez te państwa.

W żadnym razie Unia ani WP nie ponoszą odpowiedzialności wobec państw wnoszących wkład za działania lub zaniechania działań ze strony dowódcy misji UE w związku z korzystaniem ze środków finansowych udostępnionych przez te państwa.

3. KPiB zatwierdza przyjęcie wkładu finansowego państw trzecich na rzecz komórki ds. projektów.";

6) w art. 11 wprowadza się następujące zmiany:

a) w ust. 1 zdanie wprowadzające otrzymuje brzmienie: „WP jest upoważniony do udostępniania państwom trzecim, które przyłączą się do niniejszej decyzji, w stosownych przypadkach i zgodnie z potrzebami misji, informacji niejawnych UE sporządzonych do celów misji, zgodnie z decyzją Rady 2013/488/UE (*).

(*) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1)";

b) w ust. 2 i 3 wyrazy „decyzją 2011/292/UE" zastępuje się wyrazami „decyzją 2013/488/UE";

7) art.12 ust. 2 i 3 otrzymuje brzmienie:

„2. Mandat misji wojskowej UE zostaje zakończony w dniu 31 grudnia 2016 r.

3. Niniejsza decyzja traci moc z dniem zamknięcia dowództwa UE, biura łącznikowego i ds. wsparcia w Nairobi i komórki wsparcia w Brukseli, zgodnie z zatwierdzonymi planami dotyczącymi zakończenia misji wojskowej UE oraz bez uszczerbku dla procedur dotyczących kontroli i prezentacji sprawozdań finansowych misji wojskowej UE, ustanowionych w decyzji Athena.".

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Niniejszą decyzję stosuje się od dnia 1 kwietnia 2015 r.

Sporządzono w Brukseli dnia 16 marca 2015 r.

W imieniu Rady
F. MOGHERINI
Przewodniczący

DECYZJA RADY (WPZiB) 2015/442

z dnia 16 marca 2015 r.

w sprawie rozpoczęcia wojskowej misji doradczej Unii Europejskiej w dziedzinie WPBiO w Republice Środkowoafrykańskiej (EUMAM RCA) oraz zmieniająca decyzję (WPZiB) 2015/78

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 42 ust. 4 i art. 43 ust. 2,

uwzględniając decyzję Rady (WPZiB) 2015/78 z dnia 19 stycznia 2015 r. w sprawie wojskowej misji doradczej Unii Europejskiej w dziedzinie WPBiO w Republice Środkowoafrykańskiej (EUMAM RCA) ([1]), w szczególności jej art. 4,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 19 stycznia 2015 r. Rada przyjęła decyzję (WPZiB) 2015/78.

(2) W dniu 9 lutego 2015 r. Rada zatwierdziła zasady zaangażowania dla EUMAM RCA.

(3) W dniu 6 marca 2015 r. Rada zatwierdziła plan misji dla EUMAM RCA.

(4) W dniu 11 marca Komitet Polityczny i Bezpieczeństwa z zadowoleniem przyjął pismo dowódcy misji w sprawie zalecenia o rozpoczęciu EUMAM RCA oraz o planowanym czasie dotyczącym deklaracji wstępnej zdolności operacyjnej EUMAM RCA.

(5) EUMAM RCA powinna zostać rozpoczęta w dniu 16 marca 2015 r.

(6) Zgodnie z art. 5 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w opracowaniu oraz wprowadzaniu w życie decyzji i działań Unii, które mają wpływ na kwestie polityczno-obronne. W związku z tym Dania nie uczestniczy we wprowadzeniu w życie niniejszej decyzji ani nie współfinansuje niniejszej misji,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Wojskowa misja doradcza Unii Europejskiej w dziedzinie WPBiO w Republice Środkowoafrykańskiej („EUMAM RCA”) zostaje rozpoczęta w dniu 16 marca 2015 r.

Artykuł 2

Dowódca misji UE EUMAM RCA zostaje niniejszym upoważniony ze skutkiem natychmiastowym do rozpoczęcia realizacji misji.

Artykuł 3

Artykuł 4 ust. 2 decyzji (WPZiB) 2015/78 otrzymuje brzmienie:

„2. EUMAM RCA zostanie rozpoczęta decyzją Rady w dniu zaleconym przez dowódcę misji, po zatwierdzeniu planu misji oraz, w razie potrzeby, dodatkowych zasad zaangażowania.”.

([1]) Dz.U. L 13 z 20.1.2015, s. 8.

Artykuł 4

Niniejsza decyzja wchodzi w życie z dniem jej przyjęcia.

Sporządzono w Brukseli dnia 16 marca 2015 r.

W imieniu Rady
F. MOGHERINI
Przewodniczący

DECYZJA KOMISJI (UE, Euratom) 2015/443

z dnia 13 marca 2015 r.

w sprawie bezpieczeństwa w Komisji

KOMISJA EUROPEJSKA,

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

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej,

uwzględniając Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do traktatów, w szczególności jego art. 18,

a także mając na uwadze, co następuje:

(1) Zapewnienie bezpieczeństwa w obrębie Komisji ma umożliwić jej funkcjonowanie w bezpiecznym i zabezpieczonym środowisku dzięki ustanowieniu spójnego i zintegrowanego podejścia do bezpieczeństwa, utrzymaniu odpowiedniego poziomu ochrony osób, mienia i informacji współmiernie do rozpoznanego ryzyka oraz zapewnieniu bezpieczeństwa szybko i skutecznie.

(2) Komisja, podobnie jak inne organy międzynarodowe, stoi w obliczu poważnych zagrożeń i wyzwań w dziedzinie bezpieczeństwa, w szczególności, w związku z terroryzmem, atakami cybernetycznymi, szpiegostwem politycznym i handlowym.

(3) Komisja Europejska zawarła z rządami Belgii, Luksemburga i Włoch porozumienia w sprawie bezpieczeństwa swoich głównych siedzib ([1]). Porozumienia te stanowią potwierdzenie, że Komisja jest odpowiedzialna za swoje bezpieczeństwo.

(4) Aby zapewnić bezpieczeństwo osób, mienia i informacji, Komisja może być zmuszona do podjęcia działań w obszarach chronionych prawami podstawowymi sformułowanymi w Karcie praw podstawowych i w europejskiej konwencji praw człowieka i uznawanymi przez Trybunał Sprawiedliwości.

(5) Wszelkie tego typu działania powinny być zatem uzasadnione znaczeniem interesu, jaki mają za zadanie chronić, powinny być proporcjonalne i zapewniać pełne poszanowanie praw podstawowych, w tym w szczególności prawa do prywatności i ochrony danych.

(6) W ramach systemu nastawionego na praworządność i poszanowanie praw podstawowych Komisja musi dążyć do zapewnienia odpowiedniego poziomu bezpieczeństwa swoich pracowników, mienia i informacji, dzięki czemu zapewnione będzie prowadzenia działalności bez ograniczania przy tym praw podstawowych w stopniu większym niż to ściśle konieczne.

(7) Bezpieczeństwo w Komisji opiera się na zasadach legalności, przejrzystości, proporcjonalności i odpowiedzialności.

(8) Pracowników upoważnionych do podejmowania środków bezpieczeństwa nie należy stawiać w niekorzystnej sytuacji ze względu na ich działania, chyba że działania te wykraczały poza zakres ich uprawnień lub spowodowały naruszenie prawa, więc niniejszą decyzję należy uznać za instrukcję postępowania w rozumieniu regulaminu pracowniczego.

(9) Komisja powinna podjąć właściwe inicjatywy, aby promować i wzmacniać swoją kulturę bezpieczeństwa, efektywniej zapewniając bezpieczeństwo, poprawiając zarządzanie bezpieczeństwem, dalej zacieśniając sieci i współpracę z odpowiednimi organami na szczeblu międzynarodowym, europejskim i krajowym oraz poprawiając monitorowanie i kontrolę procesu wdrażania środków bezpieczeństwa.

(10) Utworzenie Europejskiej Służby Działań Zewnętrznych (ESDZ) jako funkcjonalnie autonomicznego organu Unii miało znaczący wpływ na interesy Komisji w zakresie bezpieczeństwa, w związku z tym konieczne jest, aby ESDZ i Komisja ustanowiły zasady i procedury dotyczące współpracy w zakresie bezpieczeństwa i zabezpieczenia, w szczególności w odniesieniu do wywiązywania się przez Komisję z obowiązku dochowania należytej staranności wobec własnych pracowników w delegaturach Unii.

([1]) Por. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité" z dnia 31 grudnia 2004 r., „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" z dnia 20 stycznia 2007 r. i „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" z dnia 22 lipca 1959 r.

(11) Polityka bezpieczeństwa prowadzona przez Komisję powinna być realizowana w sposób zgodny z innymi procesami i procedurami wewnętrznymi, które mogą obejmować kwestię bezpieczeństwa. Należą do nich w szczególności zarządzanie ciągłością działania, które ma na celu zachowanie funkcji krytycznych Komisji w przypadku zakłócenia działania, oraz proces ARGUS wykorzystywany do koordynacji sytuacji kryzysowych o charakterze wielosektorowym.

(12) Niezależnie od środków istniejących już w momencie przyjęcia niniejszej decyzji i zgłoszonych Europejskiemu Inspektorowi Ochrony Danych ([1]), wszelkie środki wprowadzone w ramach niniejszej decyzji i związane z przetwarzaniem danych osobowych podlegają przepisom wykonawczym zgodnie z art. 21, w którym określono odpowiednie gwarancje dla podmiotów danych.

(13) W związku z tym istnieje potrzeba dokonania przez Komisję przeglądu, aktualizacji i konsolidacji istniejącej podstawy prawnej dotyczącej bezpieczeństwa w Komisji.

(14) Należy zatem uchylić decyzję Komisji C(94) 2129 ([2]),

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

PRZEPISY OGÓLNE

Artykuł 1

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

1) „mienie" oznacza wszystkie ruchomości i nieruchomości oraz posiadłości Komisji;

2) „departament Komisji" oznacza dyrekcję generalną lub służbę Komisji lub gabinet członka Komisji;

3) „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;

4) „kontrola ryzyka" oznacza wszelkie środki bezpieczeństwa, co do których można przypuszczać, że pozwolą skutecznie kontrolować ryzyko związane z bezpieczeństwem dzięki zapobieganiu ryzyku, jego ograniczaniu, unikaniu lub przenoszeniu.

5) „sytuacja kryzysowa" oznacza okoliczność, zdarzenie, incydent lub sytuację wyjątkową (lub ich serię bądź połączenie) prowadzące do poważnego lub bezpośredniego zagrożenia dla bezpieczeństwa Komisji, niezależnie od źródła zagrożenia;

6) „dane" oznaczają informacje w formie, która pozwala na ich przekazanie, zapisanie lub przetworzenie;

7) „członek Komisji odpowiedzialny za bezpieczeństwo" oznacza członka Komisji odpowiedzialnego za Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

8) „dane osobowe" oznaczają dane osobowe w rozumieniu art. 2 lit. a) rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([3]);

9) „obiekty" oznaczają dowolną nieruchomość lub inną własność i mienie Komisji;

10) „zapobieganie ryzyku" oznacza wszelkie środki bezpieczeństwa, co do których można przypuszczać, że będą utrudniać, opóźniać lub powstrzymywać występowanie ryzyka związanego z bezpieczeństwa.

11) „ryzyko związane z bezpieczeństwem" oznacza połączenie stopnia zagrożenia, stopnia podatności na zagrożenia i ewentualnych skutków zdarzenia;

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

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Decyzja Komisji C(94) 2129 z dnia 8 września 1994 r. w sprawie zadań Biura Bezpieczeństwa.

([3]) 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).

13) „środek bezpieczeństwa" oznacza każdy środek podejmowany zgodnie z niniejszą decyzją na potrzeby skontrolowania ryzyka związanego z bezpieczeństwem;

14) „regulamin pracowniczy" oznacza Regulamin pracowniczy urzędników Unii Europejskiej ustanowiony rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 ([1]) i aktami go zmieniającymi;

15) „zagrożenie dla bezpieczeństwa" oznacza każde zdarzenie lub czynnik, co do których można przypuszczać, że negatywnie wpłyną na bezpieczeństwo, jeżeli nie spotkają się z odpowiednią reakcją i nie zostaną skontrolowane;

16) „bezpośrednie zagrożenie dla bezpieczeństwa" oznacza zagrożenie dla bezpieczeństwa, które ma miejsce bez wcześniejszego ostrzeżenia lub z wcześniejszym ostrzeżeniem wysłanym na krótko przed wystąpieniem zagrożenia, oraz

17) „poważne zagrożenie dla bezpieczeństwa" oznacza zagrożenie dla bezpieczeństwa, co do którego można przypuszczać, że doprowadzi do utraty życia, poważnego urazu lub szkody, znacznego uszkodzenia mienia, narazi na szwank bezpieczeństwo danych szczególnie chronionych, zakłóci działanie systemów IT lub istotnych zdolności operacyjnych Komisji;

18) „podatność" oznacza dowolny słaby punkt, co do którego można przypuszczać, że negatywnie wpłynie na bezpieczeństwo w Komisji, jeżeli zostanie wykorzystany przez jedno zagrożenie lub większą ich liczbę.

Artykuł 2

Przedmiot

1. W niniejszej decyzji określa się cele, podstawowe zasady, organizację i obowiązki w zakresie bezpieczeństwa w Komisji.

2. Niniejszą decyzję stosuje się do wszystkich departamentów Komisji i do wszystkich jej obiektów.Personel Komisji zatrudniony w delegaturach Unii podlegają przepisom bezpieczeństwa obowiązującym w przypadku Europejskiej Służby Działań Zewnętrznych ([2]).

3. Nie naruszając żadnych konkretnych wskazań dotyczących poszczególnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Komisji, pracowników Komisji objętych regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Unii Europejskiej, ekspertów krajowych oddelegowanych do Komisji, dostawców usług i ich pracowników, stażystów oraz do wszystkich osób mających dostęp do budynków lub innego mienia Komisji lub do informacji znajdujących się w posiadaniu Komisji.

4. Przepisy niniejszej decyzji nie naruszają decyzji Komisji 2002/47/WE, EWWiS, Euratom ([3]) i decyzji Komisji 2004/563/WE, Euratom ([4]), decyzji Komisji C(2006) 1623 ([5]) i decyzji Komisji C(2006) 3602 ([6]).

ROZDZIAŁ 2

ZASADY

Artykuł 3

Zasady dotyczące bezpieczeństwa w Komisji

1. W ramach wdrażania niniejszej decyzji Komisja postępuje zgodnie z traktatami, a w szczególności z Kartą praw podstawowych i Protokołem nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej oraz instrumentami, o których mowa w motywie 2, i wszelkimi obowiązującymi przepisami prawa krajowego, a także warunkami określonymi w niniejszej decyzji. W stosownych przypadkach wydaje się instrukcje bezpieczeństwa w rozumieniu art. 21 ust. 2 zawierające wytyczne w tym zakresie.

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

3. Zasada legalności wskazuje na konieczność ścisłego przestrzegania ram prawnych przy wdrażaniu niniejszej decyzji oraz stosowania się do wymogów prawnych.

([1]) Rozporządzenie Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiające Regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Wspólnot Europejskich oraz ustanawiające specjalne środki stosowane tymczasowo wobec urzędników Komisji (warunki zatrudnienia innych pracowników) (Dz.U. L 56 z 4.3.1968, s. 1).

([2]) Decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 19 kwietnia 2013 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych (Dz.U. C 190 z 29.6.2013, s. 1).

([3]) 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) z załączonymi przepisami dotyczącymi zarządzania dokumentami.

([4]) Decyzja Komisji 2004/563/WE, Euratom z dnia 7 lipca 2004 r. zmieniająca jej regulamin wewnętrzny (Dz.U. L 251 z 27.7.2004, s. 9) z załączonymi przepisami dotyczącymi dokumentów elektronicznych i cyfrowych.

([5]) Decyzja C(2006) 1623 z dnia 21 kwietnia 2006 r. ustanawiająca zharmonizowaną politykę bezpieczeństwa i higieny pracy dla wszystkich pracowników Komisji Europejskiej.

([6]) Decyzja C(2006) 3602 z dnia 16 sierpnia 2006 r. dotycząca bezpieczeństwa systemów informacyjnych wykorzystywanych przez Komisję Europejską.

4. Wszelkie środki bezpieczeństwa podejmuje się jawnie, chyba że istnieje uzasadnione przekonanie, że takie działanie może osłabić ich skutek. Adresatów środka bezpieczeństwa powiadamia się z wyprzedzeniem o przyczynach zastosowania środka i jego skutkach, chyba że istnieje uzasadnione przekonanie, że jego działanie zostanie osłabione w wyniku przekazania takiej informacji. W takim przypadku adresata środka bezpieczeństwa powiadamia się po wyeliminowaniu ryzyka osłabienia działania środka bezpieczeństwa.

5. Departamenty Komisji zapewniają uwzględnianie kwestii bezpieczeństwa od początku opracowywania i realizacji polityki, decyzji, programów, projektów i działań Komisji, za które są odpowiedzialne. W tym celu, od najwcześniejszych etapów przygotowań, departamenty angażują Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w ogólnym zakresie i głównego inspektora ds. bezpieczeństwa informacji w Komisji w odniesieniu do systemów IT.

6. W stosownych przypadkach Komisja dąży do nawiązania współpracy z właściwymi organami państwa przyjmującego, innych państw członkowskich i innych instytucji, agencji lub organów UE uwzględniając, w miarę możliwości, środki podejmowane lub planowane przez te organy w celu ograniczenia ryzyka związanego z bezpieczeństwem.

Artykuł 4

Obowiązek przestrzegania

1. Przestrzeganie niniejszej decyzji i jej przepisów wykonawczych oraz środków bezpieczeństwa i instrukcji udzielonych przez upoważnionych pracowników jest obowiązkowe.

2. Nieprzestrzeganie przepisów bezpieczeństwa może pociągać za sobą odpowiedzialność dyscyplinarną zgodnie z traktatami i regulaminem pracowniczym oraz sankcje umowne lub czynności prawne na mocy krajowych przepisów ustawowych i wykonawczych.

ROZDZIAŁ 3

ZAPEWNIENIE BEZPIECZEŃSTWA

Artykuł 5

Upoważnieni pracownicy

1. Jedynie pracownikom upoważnionym na podstawie imiennego uprawnień przyznanych im przez Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa, z uwagi na ich bieżące obowiązki, można przyznać prawo do stosowania jednego lub kilku z następujących środków:

1) noszenie broni bocznej;

2) prowadzenie dochodzeń w sprawie bezpieczeństwa, o których mowa w art. 13;

3) podejmowanie środków bezpieczeństwa, o których mowa w art. 12, określonych w uprawnieniu.

2. Uprawnienia, o których mowa w ust. 1, przyznaje się na okres nie dłuższy niż okres zajmowania przez daną osobę stanowiska lub pełnienia przez nią określonej funkcji, w odniesieniu do której przyznano dane uprawnienie. Uprawnienia przyznaje się zgodnie z obowiązującymi przepisami określonymi w art. 3 ust. 1.

3. Jeżeli chodzi o upoważnionych pracowników, niniejsza decyzja stanowi instrukcję postępowania w rozumieniu art. 21 regulaminu pracowniczego.

Artykuł 6

Przepisy ogólne dotyczące środków bezpieczeństwa

1. Podejmując środki bezpieczeństwa Komisja przede wszystkim, na ile to możliwe, zapewnia:

a) poszukiwanie wsparcia lub pomocy ze strony danego państwa, pod warunkiem że państwo to jest państwem członkowskim Unii Europejskiej, a jeżeli nie, to jest stroną europejskiej konwencji praw człowieka lub gwarantuje prawa, które są co najmniej równorzędne prawom zagwarantowanym w tej konwencji;

b) przekazanie informacji na temat danej osoby jedynie odbiorcom innym niż instytucje i organy wspólnotowe niepodlegające prawu krajowemu przyjętemu zgodnie z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady ([1]), zgodnie z art. 9 rozporządzenia (WE) nr 45/2001;

([1]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

c) jeżeli dana osoba stanowi zagrożenie dla bezpieczeństwa, wobec tej osoby stosuje się wszelkie środki bezpieczeństwa oraz można ją obciążyć poniesionymi kosztami. Wymienione środki bezpieczeństwa można zastosować wobec innych osób tylko wówczas, jeżeli bezpośrednie lub poważne zagrożenie dla bezpieczeństwa jest kontrolowane i spełnione zostały następujące warunki:

   a) nie można podjąć przewidzianych środków wobec osoby stwarzającej zagrożenie dla bezpieczeństwa lub istnieje prawdopodobieństwo, że dane środki będą nieskuteczne;

   b) Komisja nie może kontrolować zagrożenia dla bezpieczeństwa w ramach swoich działań, ani nie może tego dokonać w odpowiednim czasie;

   c) środek nie stanowi nieproporcjonalnego zagrożenia dla innej osoby i jej praw.

2. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa ustanawia przegląd środków bezpieczeństwa, w przypadku których konieczne może być orzeczenie sądu zgodne z przepisami ustawowymi i wykonawczymi państw członkowskich, w których znajdują się obiekty Komisji.

3. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zwrócić się do wykonawcy o wykonanie, pod kierownictwem i nadzorem Dyrekcji ds. Bezpieczeństwa, zadań związanych z bezpieczeństwem.

Artykuł 7

Środki bezpieczeństwa w odniesieniu do osób

1. Uwzględniając wymogi w zakresie bezpieczeństwa, osobom przebywającym w obiektach Komisji przysługuje odpowiedni poziom ochrony.

2. W przypadku poważnego ryzyka związanego z bezpieczeństwem Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa zapewnia ścisłą ochronę członkom Komisji lub innym pracownikom, w sytuacji, gdy z oceny zagrożenia wynika, że taka ochrona jest potrzebna, aby zapewnić im bezpieczeństwo.

3. W przypadku poważnego ryzyka związanego z bezpieczeństwem Komisja może zarządzić ewakuację swoich obiektów.

4. Ofiary wypadków lub ataków na terenie obiektów Komisji otrzymają pomoc.

5. Aby zapobiegać ryzyku związanemu z bezpieczeństwem i kontrolować je, upoważnieni pracownicy mogą dokonać kontroli przeszłości osób objętych zakresem niniejszej decyzji w celu ustalenia, czy przyznanie takim osobom dostępu do obiektów Komisji lub jej informacji nie stanowi zagrożenia dla bezpieczeństwa. W tym celu oraz zgodnie z rozporządzeniem (WE) nr 45/2001 i przepisami, o których mowa w art. 3 ust. 1, upoważnieni pracownicy mogą:

a) korzystać z wszelkich dostępnych Komisji źródeł informacji, uwzględniając wiarygodność źródła informacji;

b) uzyskać dostęp do akt personalnych lub danych Komisji na temat osób, które zatrudnia lub planuje zatrudnić, lub na temat pracowników wykonawców, gdy jest to należycie uzasadnione.

Artykuł 8

Środki bezpieczeństwa w odniesieniu do bezpieczeństwa fizycznego i mienia

1. Bezpieczeństwo mienia zapewnia się w wyniku zastosowania odpowiednich fizycznych i technicznych środków ochronnych i odpowiednich procedur, zwanych dalej „bezpieczeństwem fizycznym", tworzących wielowarstwowy system.

2. Środki można przyjąć zgodnie z niniejszym artykułem w celu ochrony osób lub informacji w Komisji oraz ochrony mienia.

3. Cele bezpieczeństwa fizycznego obejmują:

— zapobieganie aktom przemocy wymierzonym w członków Komisji lub osoby objęte zakresem niniejszej decyzji,

— zapobieganie szpiegostwu i stosowaniu podsłuchu w celu zdobycia danych szczególnie chronionych lub informacji niejawnych,

— zapobieganie kradzieżom, aktom wandalizmu, sabotażowi i innym aktom przemocy zmierzającym do uszkodzenia lub zniszczenia budynków i mienia Komisji,

— umożliwienie prowadzenia dochodzenia wyjaśniającego i dochodzenia w sprawie bezpieczeństwa w zakresie incydentów związanych z bezpieczeństwem, w tym w drodze sprawdzenia plików dziennika kontroli wejść i wyjść, nagrań w systemie CCTV, zapisów rozmów telefonicznych i podobnych danych, o których mowa w art. 22 ust. 2 poniżej i innych źródłach informacji.

4. Bezpieczeństwo fizyczne obejmuje:

— politykę dostępu mającą zastosowanie do wszystkich osób lub pojazdów potrzebujących dostępu do obiektów Komisji, w tym parkingów,

— system kontroli dostępu, który tworzą strażnicy, urządzenia i środki techniczne, systemy informacyjne lub połączenie wszystkich tych elementów.

5. W celu zapewnienia bezpieczeństwa fizycznego mogą zostać podjęte następujące działania:

— rejestrowanie wejść i wjazdów na teren obiektów Komisji oraz wyjść i wyjazdów z terenu Komisji w odniesieniu do osób, pojazdów, towarów i urządzeń,

— kontrole tożsamości w obiektach,

— kontrole pojazdów, towarów i urządzeń za pomocą środków wizualnych lub technicznych,

— zapobieganie wejścia, wjazdu i wwozu nieupoważnionych osób, pojazdów i towarów na teren obiektów Komisji.

Artykuł 9

Środki bezpieczeństwa w odniesieniu do informacji

1. Bezpieczeństwo informacji obejmuje wszystkie informacje będące w posiadaniu Komisji.

2. Bezpieczeństwo informacji, niezależnie od swojej formy, utrzymuje równowagę między przejrzystością, proporcjonalnością, odpowiedzialnością i skutecznością a koniecznością ochrony informacji przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zniszczeniem lub nieuprawnioną zmianą.

3. Bezpieczeństwo informacji ma na celu ochronę poufności, integralności i dostępności.

4. W związku z tym stosuje się procesy zarządzania ryzykiem w celu sklasyfikowania zasobów informacyjnych i opracowania proporcjonalnych środków bezpieczeństwa, procedur i norm, w tym środków zmniejszających ryzyko.

5. Te ogólne zasady dotyczące bezpieczeństwa informacji stosuje się w szczególności w odniesieniu do:

a) „informacji niejawnych UE" (zwanych dalej „EUCI"), a mianowicie wszelkich informacji lub materiałów objętych klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu zaszkodzić interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego;

b) „szczególnie chronionych informacji jawnych", tj. informacji lub materiałów, które Komisja musi chronić z powodu zobowiązań prawnych określonych w traktatach lub aktach przyjętych w celu ich wykonania lub ze względu na ich szczególną ochronę. Szczególnie chronione informacje jawne obejmują między innymi informacje lub materiały objęte ze względu na swój charakter tajemnicą służbową, o czym jest mowa w art. 339 TFUE, informacje objęte interesami chronionymi na mocy art. 4 rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiej i Rady ([1]) w związku z odpowiednim orzecznictwem Trybunału Sprawiedliwości lub dane osobowe objęte zakresem rozporządzenia (WE) nr 45/2001.

6. Szczególnie chronione informacje jawne podlegają zasadom dotyczącym przetwarzania tych informacji i ich przechowywania. Informacje te ujawnia się tylko tym osobom, które muszą je znać. W razie konieczności zapewnienia skutecznej ochrony poufności informacji, stosuje się oznaczenie identyfikujące dokument niejawny i odpowiednie instrukcje przetwarzania zatwierdzone przez Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa. Jeżeli informacje tego rodzaju przetwarza się lub przechowuje w systemach teleinformatycznych, wówczas chroni się je także zgodnie z decyzją C(2006) 3602, jej przepisami wykonawczymi i odpowiednimi normami.

7. Wobec każdej osoby odpowiedzialnej za narażenie na szwank bezpieczeństwa lub utratę EUCI lub szczególnie chronionych informacji jawnych, które są określone jako takie w zasadach dotyczących ich przetwarzanie i przechowywanie, może zostać wszczęte postępowanie dyscyplinarne zgodnie z regulaminem pracowniczym. Postępowanie dyscyplinarne nie wpływa na wszelkie dalsze postępowania sądowe lub karne prowadzone przez właściwe organy krajowe państw członkowskich zgodnie z ich przepisami ustawowymi i wykonawczymi oraz na umowne środki odwoławcze.

([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).

Artykuł 10

Środki bezpieczeństwa w odniesieniu do systemów teleinformatycznych

1. Wszystkie systemy teleinformatyczne („CIS") wykorzystywane przez Komisję są zgodne z polityką Komisji w dziedzinie bezpieczeństwa systemów informatycznych określoną w decyzji C(2006) 3602, jej przepisach wykonawczych i odpowiednich normach bezpieczeństwa.

2. Służby Komisji posiadające system teleinformatyczny, zarządzające nim lub obsługujące go zezwalają na dostęp do tych systemów wyłącznie innym instytucjom, agencjom, organom UE lub innym organizacjom, pod warunkiem że wspomniane instytucje, agencje, organy UE lub inne organizacje mogą zagwarantować wystarczającą pewność, że ich systemy IT są chronione na poziomie równorzędnym polityce Komisji w dziedzinie bezpieczeństwa systemów informatycznych określonej w decyzji C(2006) 3602, jej przepisach wykonawczych i odpowiednich normach bezpieczeństwa. Komisja monitoruje przestrzeganie polityki, a w przypadku poważnego naruszenia lub utrzymującego się nieprzestrzegania jest uprawniona do zakazania dostępu.

Artykuł 11

Analiza kryminalistyczna dotycząca bezpieczeństwa cybernetycznego

Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest przede wszystkim odpowiedzialna za przeprowadzenia technicznej analizy kryminalistycznej we współpracy z właściwymi departamentami Komisji w celu wsparcia dochodzeń w sprawie bezpieczeństwa, o których mowa w art. 13, związanych z kontrwywiadem, przeciekiem danych, atakami cybernetycznymi i bezpieczeństwem systemów informatycznych.

Artykuł 12

Środki bezpieczeństwa w odniesieniu do osób i przedmiotów

1. W celu zapewnienia bezpieczeństwa w Komisji oraz zapobiegania ryzyku i jego kontroli upoważnieni pracownicy mogą, zgodnie z art. 5 oraz przestrzegając zasad określonych w art. 3, zastosować m.in. jeden lub kilka środków bezpieczeństwa, takich jak:

a) zabezpieczenie miejsca i dowodów, w tym plików dziennika kontroli wyjść i wejść, nagrań w systemie CCTV, w przypadku incydentów lub zachowań, które mogą prowadzić do wszczęcia postępowania administracyjnego, dyscyplinarnego, cywilnego lub karnego;

b) ograniczone środki dotyczące osób stwarzających zagrożenie dla bezpieczeństwa, w tym nakazanie opuszczenia obiektów Komisji, eskortowanie podczas opuszczania obiektów Komisji, zakazanie wstępu do obiektów Komisji przez określony czas; przy czym ten ostatni środek określa się zgodnie z kryteriami, które mają zostać zdefiniowane w przepisach wykonawczych;

c) ograniczone środki dotyczące przedmiotów stwarzających zagrożenie dla bezpieczeństwa, w tym usunięcie, zajęcie lub unieszkodliwienie przedmiotów;

d) przeszukanie obiektów Komisji, w tym biur, na terenie tych obiektów;

e) przeszukanie CIS i urządzeń, przesyłu danych telefonicznych i telekomunikacyjnych, plików dzienników, kont użytkowników itd.;

f) inne szczególne środki bezpieczeństwa o podobnych skutkach, mające na celu zapobieganie ryzyku związanemu z bezpieczeństwem lub kontrolę takiego ryzyka, w szczególności w kontekście praw Komisji jako właściciela lub pracodawcy zgodnie z mającym zastosowanie prawem krajowym.

2. W wyjątkowych okolicznościach pracownicy Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa upoważnieni zgodnie z art. 5 mogą podjąć wszelkie środki ochronne, ściśle przestrzegając zasad określonych w art. 3. Jak najszybciej po zastosowaniu środków, pracownicy powiadamiają dyrektora Dyrekcji ds. Bezpieczeństwa, który występuje o odpowiednie upoważnienie do Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa potwierdzające zastosowane środki i zezwalające na podjęcie dalszych niezbędnych działań oraz kontaktuje się w stosownych przypadkach z właściwymi organami krajowymi.

3. Zgodnie z niniejszym artykułem środki bezpieczeństwa należy udokumentować w czasie ich stosowania lub, w przypadku bezpośredniego zagrożenia lub sytuacji kryzysowej, w rozsądnym terminie po ich podjęciu. W tym ostatnim przypadku dokumentacja musi także zawierać elementy, na których opierała się ocena dotycząca zaistnienia bezpośredniego zagrożenia lub sytuacji kryzysowej. Dokumentacja może być zwięzła, ale powinna być tworzona w taki sposób, aby osoba objęta środkiem mogła skorzystać z prawa do obrony i ochrony danych osobowych zgodnie z rozporządzeniem (WE) nr 45/2001 oraz, aby możliwa była kontrola legalności danego środka. Akta personalne osoby nie zawierają żadnych informacji na temat szczególnych środków bezpieczeństwa zastosowanych wobec pracownika.

4. Stosując środki bezpieczeństwa zgodnie z lit. b), Komisja gwarantuje także, że dana osoba będzie miała możliwość skontaktowania się z prawnikiem lub zaufaną osobą oraz zostanie poinformowana o przysługującym jej prawie do odwołania się do Europejskiego Inspektora Ochrony Danych.

Artykuł 13

Dochodzenia

1. 1. Bez uszczerbku dla art. 86 i załącznika IX do regulaminu pracowniczego i dla wszelkich szczególnych ustaleń między Komisją a ESDZ, takich jak szczególne ustalenia podpisane w dniu 28 maja 2014 r. między Dyrekcją Generalną Zasobów Ludzkich i Bezpieczeństwa Komisji Europejskiej a Europejską Służbą Działań Zewnętrznych w sprawie obowiązku dochowania należytej staranności wobec personelu Komisji oddelegowanego do delegatur Unii, można prowadzić dochodzenia w sprawie bezpieczeństwa:

a) w przypadku incydentów mających wpływ na bezpieczeństwo w Komisji, w tym podejrzeń o popełnienie przestępstwa;

b) w przypadku potencjalnego wycieku szczególnie chronionych informacji jawnych, EUCI lub informacji niejawnych Euratom, nieostrożnego obchodzenia się z tymi informacjami lub narażenia ich na szwank;

c) w kontekście kontrwywiadu i walki z terroryzmem;

d) w przypadku poważnych incydentów cybernetycznych.

2. Decyzję o przeprowadzeniu dochodzenia w sprawie bezpieczeństwa podejmuje Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa, który będzie jednocześnie odbiorcą sprawozdania z dochodzenia.

3. Dochodzenia w sprawie bezpieczeństwa prowadzone są jedynie przez wyznaczonych i należycie upoważnionych zgodnie z art. 5 pracowników Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa.

4. Upoważnieni pracownicy korzystają w sposób niezależny ze swoich uprawnień w zakresie prowadzenia dochodzenia w sprawie bezpieczeństwa zgodnie z upoważnieniem i posiadają uprawnienia wymienione w art. 12.

5. Upoważnieni pracownicy posiadający uprawnienia do prowadzenia dochodzeni w sprawie bezpieczeństwa mogą gromadzić informacje pochodzące ze wszystkich dostępnych źródeł na temat wszelkich przestępstw administracyjnych lub kryminalnych popełnionych na terenie obiektu Komisji lub z udziałem osób wymienionych w art. 2 ust. 3 w roli ofiary lub sprawcy tych przestępstw.

6. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa powiadamia właściwe organy przyjmującego państwa członkowskiego lub w stosownych przypadkach innego państwa członkowskiego, w szczególności gdy z dochodzenia wynika, że doszło do popełnienia przestępstwa. W tym kontekście Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa może w stosownych przypadkach, lub gdy jest to wymagane, zapewnić wsparcie organom przyjmującego państwa członkowskiego lub innego państwa członkowskiego.

7. W przypadku poważnych incydentów cybernetycznych Dyrekcja Generalna ds. Informatyki współpracuje ściśle z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu zapewnienia wsparcia we wszystkich kwestiach technicznych. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa podejmuje w porozumieniu z Dyrekcją Generalną ds. Informatyki decyzję, kiedy należy powiadomić właściwe organy państwa przyjmującego lub innego państwa członkowskiego. Służby koordynacji incydentów zespołu reagowania na incydenty komputerowe obsługującego instytucje, organy i agencje europejskie („CERT-EU") będzie wykorzystywana w celu zapewnienia wsparcia pozostałym narażonym instytucjom i agencjom UE.

8. Dochodzenia w sprawie bezpieczeństwa należy udokumentować.

Artykuł 14

Wyznaczenie kompetencji w odniesieniu do postępowania sprawdzającego/dochodzenia w sprawie bezpieczeństwa i innych rodzajów dochodzeń

1. Jeżeli Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa prowadzi dochodzenia w sprawie bezpieczeństwa, o których mowa w art. 13, i jeżeli przedmiotowe dochodzenia wchodzą w zakres kompetencji Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) lub Biura Dochodzeń i Postępowań Dyscyplinarnych Komisji (IDOC), wówczas bezzwłocznie kontaktuje się z tymi organami, w szczególności aby nie narazić na szwank późniejszych działań podejmowanych przez OLAF lub IDOC. W stosownych przypadkach Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa zwraca się do OLAF-u i IDOC-u o przystąpienie do udziału w dochodzeniu.

2. Dochodzenia w sprawie bezpieczeństwa, o których mowa w art. 13, pozostają bez uszczerbku dla kompetencji OLAF-u i IDOC-u określonych w przepisach dotyczących tych organów. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zostać poproszona o udzielenie pomocy technicznej w prowadzeniu dochodzeń wszczętych przez OLAF lub IDOC.

3. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zostać poproszona o udzielenie pomocy pracownikom OLAF-u, gdy wchodzą na teren obiektów Komisji zgodnie z art. 3 ust. 5 i art. 4 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([1]), aby ułatwić im

([1]) 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).

wykonanie zadań. Dyrekcja ds. Bezpieczeństwa powiadamia o takich wnioskach o udzielenie pomocy Sekretarza Generalnego i Dyrektora Generalnego Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa lub, jeżeli takie dochodzenie prowadzone jest w obiektach Komisji zajmowanych przez jej członków lub przez sekretarza generalnego, przewodniczącego Komisji i komisarza ds. zasobów ludzkich.

4. Bez uszczerbku dla art. 22 lit. a) regulaminu pracowniczego, jeżeli sprawa może wchodzić w zakres kompetencji zarówno Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, jak i IDOC-u, Dyrekcja ds. Bezpieczeństwa doradza Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa na jak najwcześniejszym etapie w momencie przekazania przez nią informacji zgodnie z art. 13, czy istnieją podstawy, które uzasadniają udział IDOC w tej sprawie. Etap ten zostaje w szczególności uznany za zrealizowany, gdy bezpośrednie zagrożenie dla bezpieczeństwa zostanie zażegnane. Decyzję w tej sprawie podejmuje Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa.

5. W przypadku gdy sprawa może wchodzić w zakres kompetencji zarówno Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, jak i OLAF-u, Dyrekcja ds. Bezpieczeństwa niezwłocznie przekazuje informacje Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa oraz na jak najwcześniejszym etapie powiadamia Dyrektora Generalnego OLAF-u. Etap ten zostaje w szczególności uznany za zrealizowany, gdy bezpośrednie zagrożenie dla bezpieczeństwa zostanie zażegnane.

Artykuł 15

Kontrole bezpieczeństwa

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przeprowadza kontrole bezpieczeństwa, aby sprawdzić, czy służby Komisji i poszczególne osoby przestrzegają postanowień niniejszej decyzji i jej przepisów wykonawczych, oraz aby sformułować zalecenia, gdy uzna to za konieczne.

2. W stosownych przypadkach Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przeprowadza kontrole bezpieczeństwa lub wizyty monitorujące lub oceniające, aby sprawdzić, czy bezpieczeństwo służb Komisji, jej mienia i informacji, za które odpowiedzialność ponoszą inne instytucje, agencje lub organy unijne, państwa członkowskie, państwa trzecie lub organizacje międzynarodowe, jest odpowiednio chronione zgodnie z przepisami bezpieczeństwa, regulacjami i normami, które są co najmniej równorzędne przepisom, regulacjom i normom Komisji. W stosownych przypadkach i w duchu dobrej współpracy między administracjami, wspomniane kontrole bezpieczeństwa obejmują także kontrole prowadzone w kontekście wymiany informacji niejawnych z innymi instytucjami, organami i agencjami unijnymi, państwami członkowskimi lub państwami trzecimi lub organizacjami międzynarodowymi.

3. Niniejszy artykuł jest wykonywany odpowiednio w odniesieniu do personelu Komisji w delegaturach Unii, bez uszczerbku dla wszelkich szczególnych ustaleń między Komisją a ESDZ, takich jak szczególne ustalenia podpisane w dniu 28 maja 2014 r. między Dyrekcją Generalną Zasobów Ludzkich i Bezpieczeństwa Komisji Europejskiej a Europejską Służbą Działań Zewnętrznych w sprawie obowiązku dochowania należytej staranności wobec personelu Komisji oddelegowanego do delegatur Unii.

Artykuł 16

Stopnie alarmowe i zarządzanie sytuacjami kryzysowymi

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest odpowiedzialna za wdrożenie odpowiednich środków w zakresie stopni alarmowych w przewidywaniu zagrożeń i incydentów mających wpływ na bezpieczeństwo w Komisji lub w odpowiedzi na takie zagrożenia i incydenty oraz jest odpowiedzialna za środki wymagane do zarządzania sytuacjami kryzysowymi.

2. Środki w zakresie stopni alarmowych, o których mowa w ust. 1, są współmierne do poziomu zagrożenia dla bezpieczeństwa. Poziomy stopni alarmowych określa się w ścisłej współpracy z właściwymi służbami innych instytucji, agencji i organów unijnych oraz służbami państwa członkowskiego lub państw członkowskich, w których znajdują się obiekty Komisji.

3. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest punktem kontaktowym, jeżeli chodzi o stopnie alarmowe i zarządzanie sytuacjami kryzysowymi.

ROZDZIAŁ 4

ORGANIZACJA

Artykuł 17

Ogólne obowiązki służb Komisji

1. Obowiązki Komisji, o których mowa w niniejszej decyzji, są wykonywane przez Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa z upoważnienia członka Komisji odpowiedzialnego za bezpieczeństwo i na jego odpowiedzialność.

2. Szczególne ustalenia dotyczące bezpieczeństwa cybernetycznego określono w decyzji C(2006) 3602.

3. Obowiązki w zakresie wykonania niniejszej decyzji i jej przepisów wykonawczych oraz zachowania bieżącej zgodności można przekazać innym departamentom Komisji, gdy zdecentralizowany system zapewniania bezpieczeństwa przynosi znaczące oszczędności wynikające z poprawy efektywności oraz oszczędności zasobów i czasu np. ze względu na lokalizację geograficzną danych usług.

4. W przypadkach, w których zastosowanie ma ust. 3, Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, a w stosownym przypadku Dyrektor Generalny ds. Informatyki zawierają porozumienia z poszczególnymi departamentami Komisji, ustanawiając wyraźne role i obowiązki w zakresie wdrażania i monitorowania polityki bezpieczeństwa.

Artykuł 18

Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada w szczególności za:

1) opracowywanie polityki bezpieczeństwa Komisji, przepisów wykonawczych i instrukcji bezpieczeństwa;

2) gromadzenie informacji, biorąc pod uwagę ocenę zagrożeń i ryzyka związanego z bezpieczeństwem oraz informacji na temat wszystkich kwestii, które mogą wpłynąć na bezpieczeństwo w Komisji;

3) zapewnienie ochrony przed inwigilacją elektroniczną i ochrony wszystkich obiektów Komisji, z należytym uwzględnieniem ocen zagrożeń i dowodów na prowadzenie nielegalnych działań wobec interesów Komisji;

4) zapewnienie służby ratunkowej w służbach Komisji działającej 7 dni w tygodniu i 24 godziny na dobę oraz pracowników odpowiedzialnych za wszelkie kwestie związane z bezpieczeństwem;

5) wdrażanie środków bezpieczeństwa służących ograniczeniu ryzyka dla bezpieczeństwa oraz opracowywanie i prowadzenie odpowiedniego CIS w celu zaspokojenia swoich potrzeb operacyjnych, w szczególności w dziedzinach kontroli dostępu fizycznego, zarządzania upoważnieniami w zakresie bezpieczeństwa i zarządzania informacjami szczególnie chronionymi i niejawnymi UE;

6) podnoszenie świadomości, organizowanie ćwiczeń oraz zapewnianie szkoleń i doradztwa w zakresie wszystkich kwestii związanych z bezpieczeństwem w Komisji w celu promowania kultury bezpieczeństwa i utworzenia grupy pracowników odpowiednio przeszkolonych w sprawach bezpieczeństwa.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, bez uszczerbku dla kompetencji i obowiązków służb Komisji, zapewnia zewnętrzne kontakty:

1) z departamentami bezpieczeństwa innych instytucji, agencji i organów UE w sprawach związanych z bezpieczeństwem osób, mienia i informacji w Komisji;

2) ze służbami bezpieczeństwa, służbami wywiadowczymi i służbami odpowiedzialnymi za ocenę zagrożeń, w tym krajowymi organami bezpieczeństwa, służbami państw członkowskich, państw trzecich oraz organizacji i organów międzynarodowych w sprawach mających wpływ na bezpieczeństwo osób, mienia i informacji w Komisji;

3) z policją i innymi służbami ratowniczymi we wszystkich rutynowych i nadzwyczajnych sprawach mających wpływ na bezpieczeństwo Komisji;

4) z organami bezpieczeństwa innych instytucji, agencji i organów UE, państw członkowskich i państw trzecich w zakresie reagowania na ataki cybernetyczne mające potencjalny wpływ na bezpieczeństwo w Komisji;

5) w zakresie przyjmowania, oceniania i przekazywania danych wywiadowczych na temat zagrożeń stwarzanych przez działalność terrorystyczną i szpiegowską mającą wpływ na bezpieczeństwo w Komisji;

6) w zakresie kwestii związanych z informacjami niejawnymi określonymi w decyzji Komisji (UE, Euratom) 2015/444 ([1]).

3. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada w szczególności za bezpieczne przekazanie informacji zgodnie z niniejszym artykułem, w tym przekazywanie danych osobowych.

Artykuł 19

Grupa Ekspertów ds. Bezpieczeństwa Komisji

Powołuje się Grupę Ekspertów ds. Bezpieczeństwa Komisji upoważnioną do doradzania Komisji w stosownych przypadkach w sprawach związanych z polityką bezpieczeństwa wewnętrznego Komisji, a zwłaszcza w celu ochrony informacji niejawnych UE.

([1]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (zob. s. 53 niniejszego Dziennika Urzędowego).

Artykuł 20

Lokalni pełnomocnicy ochrony (LSO)

1. Każdy departament Komisji lub Gabinet wyznacza lokalnego pełnomocnika ochrony (LSO), który pełni funkcję głównego punktu kontaktowego między ich służbami a Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa we wszystkich sprawach związanych z bezpieczeństwem w Komisji. W stosownych przypadkach można wyznaczyć jednego lub kilku zastępców LSO. LSO jest urzędnikiem lub pracownikiem zatrudnionym na czas określony.

2. Jako główny punkt kontaktowy ds. bezpieczeństwa w swoim departamencie Komisji lub gabinecie, LSO przekazuje, w regularnych odstępach czasu, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa i swoim zwierzchnikom sprawozdanie na temat kwestii bezpieczeństwa dotyczących jego departamentu Komisji oraz przekazuje niezwłocznie sprawozdanie na temat wszelkich incydentów związanych z bezpieczeństwem, w tym incydentów dotyczących naruszenia EUCI lub szczególnie chronionych informacji jawnych.

3. W sprawach związanych z bezpieczeństwem systemów teleinformatycznych, LSO kontaktuje z lokalnym pełnomocnikiem bezpieczeństwa teleinformatycznego (LISO) ze swojego departamentu Komisji, którego rolę i obowiązki określono w decyzji C(2006) 3602.

4. LSO uczestniczy w szkoleniach w zakresie bezpieczeństwa i działaniach uświadamiających mających na celu zaspokojenie określonych potrzeb pracowników, wykonawców i innych osób pracujących pod zwierzchnictwem jego departamentu Komisji.

5. Na wniosek Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa LSO mogą zostać przypisane konkretne zadania w przypadku poważnego lub bezpośredniego zagrożenia dla bezpieczeństwa lub w sytuacjach wyjątkowych. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa powiadamia o tych konkretnych zadaniach Dyrektora Generalnego lub Dyrektora ds. Zasobów Ludzkich lokalnej dyrekcji generalnej LSO.

6. Obowiązki LSO pozostają bez uszczerbku dla roli i obowiązków przypisanych lokalnym pełnomocnikom bezpieczeństwa teleinformatycznego (LISO), kierownikom ds. bezpieczeństwa i higieny pracy, urzędnikom kontroli kancelarii lub wszelkim innym pracownikom pełniącym funkcje powiązane z odpowiedzialnością w zakresie bezpieczeństwa. LSO kontaktuje z nimi w celu zapewnienia spójnego i konsekwentnego podejścia do bezpieczeństwa i efektywnego przepływu informacji w sprawach związanych z bezpieczeństwem w Komisji.

7. LSO ma bezpośredni dostęp do swojego dyrektora generalnego lub szefa służby podczas informowania swojego bezpośredniego przełożonego. LSO posiada upoważnienie w zakresie bezpieczeństwa umożliwiające mu dostęp do EUCI, co najmniej do poziomu SECRET UE/EU SECRET.

8. Aby promować wymianę informacji i najlepszych praktyk Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa organizuje co najmniej dwa razy w roku konferencję LSO. Obecność osób pełniących funkcję LSO na tych konferencjach jest obowiązkowa.

ROZDZIAŁ 5

WDRAŻANIE

Artykuł 21

Przepisy wykonawcze i instrukcje bezpieczeństwa

1. W stosownych przypadkach przyjęcie przepisów wykonawczych do niniejszej decyzji w pełnej zgodności z regulaminem wewnętrznym będzie przedmiotem odrębnej decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa.

2. Po uzyskaniu uprawnień w następstwie wyżej wspomnianej decyzji Komisji członek Komisji odpowiedzialny za kwestie bezpieczeństwa może opracowywać instrukcje bezpieczeństwa, w których określi wytyczne dotyczące bezpieczeństwa i najlepsze praktyki w zakresie niniejszej decyzji i jej przepisów wykonawczych.

3. Komisja może przekazać zadania wspomniane w ust. 1 i 2 niniejszego artykułu Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa w ramach osobnej decyzji w sprawie przekazywania zadań w pełnej zgodności z regulaminem wewnętrznym.

ROZDZIAŁ 6

PRZEPISY RÓŻNE I KOŃCOWE

Artykuł 22

Przetwarzanie danych osobowych

1. Komisja przetwarza dane osobowe niezbędne do wykonania niniejszej decyzji zgodnie z rozporządzeniem (WE) nr 45/2001.

2. Niezależnie od środków istniejących już w momencie przyjęcia niniejszej decyzji i zgłoszonych Europejskiemu Inspektorowi Ochrony Danych ([1]) wszelkie środki wprowadzone w ramach niniejszej decyzji i związane z przetwarzaniem danych osobowych, takich jak pliki dziennika wejść i wyjść, nagrania w systemie CCTV, zapisy połączeń telefonicznych z biurem lub centralami wysyłkowymi i innych podobnych danych, które są wymagane ze względów bezpieczeństwa lub reagowania kryzysowego, podlegają przepisom wykonawczym zgodnie z art. 21, w którym określono odpowiednie gwarancje dla podmiotów danych.

3. Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada za bezpieczne przetwarzanie danych osobowych prowadzone w kontekście niniejszej decyzji.

4. Powyższe przepisy i procedury wykonawcze przyjmuje się po konsultacji z inspektorem ochrony danych i Europejskim Inspektorem Ochrony Danych zgodnie z rozporządzeniem (WE) nr 45/2001.

Artykuł 23

Przejrzystość

Niniejsza decyzja i jej przepisy wykonawcze są podawane do wiadomości pracowników Komisji i wszystkich osób, do których się odnoszą.

Artykuł 24

Uchylenie poprzednich decyzji

Uchyla się decyzję C(94) 2129.

Artykuł 25

Wejście w życie

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

Sporządzono w Brukseli dnia 13 marca 2015 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

DECYZJA KOMISJI (UE, Euratom) 2015/444

z dnia 13 marca 2015 r.

w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE

KOMISJA EUROPEJSKA,

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

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej, w szczególności jego art. 106,

uwzględniając Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do traktatów, w szczególności jego art. 18,

a także mając na uwadze, co następuje:

(1) Należy dokonać przeglądu i aktualizacji przepisów Komisji regulujących kwestie bezpieczeństwa i dotyczących ochrony informacji niejawnych UE (EUCI), uwzględniając zmiany instytucjonalne, organizacyjne, operacyjne i technologiczne.

(2) Komisja Europejska zawarła z rządami Belgii, Luksemburga i Włoch porozumienia w sprawie bezpieczeństwa swoich głównych siedzib ([1]).

(3) Komisja, Rada i Europejska Służba Działań Zewnętrznych są zdecydowane stosować równorzędne standardy bezpieczeństwa w celu ochrony EUCI.

(4) Ważne jest, aby w stosownych przypadkach Parlament Europejski i inne instytucje, agencje, organy lub biura UE przestrzegały zasad, standardów i przepisów dotyczących ochrony informacji niejawnych, niezbędnych do ochrony interesów Unii i jej państw członkowskich.

(5) Zarządzanie ryzykiem w odniesieniu do EUCI to zarządzanie określonym procesem. Proces ten jest ukierunkowany na określenie znanych rodzajów ryzyka związanego z bezpieczeństwem, zdefiniowanie środków bezpieczeństwa służących ograniczeniu tego ryzyka do akceptowalnego poziomu zgodnie z podstawowymi zasadami i minimalnymi standardami bezpieczeństwa określonymi w niniejszej decyzji oraz na zastosowanie tych środków zgodnie z koncepcją ochrony w głąb. Skuteczność takich środków jest poddawana ciągłej ocenie.

(6) W obrębie Komisji bezpieczeństwo fizyczne mające na celu ochronę informacji niejawnych oznacza stosowanie fizycznych i technicznych środków ochronnych, których celem jest uniemożliwienie nieuprawnionego dostępu do EUCI.

(7) Zarządzanie EUCI polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w rozdziałach 2, 3 i 5 niniejszej decyzji, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank lub utraty tych informacji, w wykrywaniu takich przypadków i usuwaniu ich skutków. Środki takie dotyczą w szczególności wytwarzania, przechowywania, rejestrowania, kopiowania, tłumaczenia, obniżania klauzuli tajności i znoszenia tej klauzuli, przemieszczania i niszczenia EUCI oraz uzupełniają ogólne przepisy Komisji dotyczące zarządzania dokumentami (decyzja 2002/47/WE ([2]), EWWiS, Euratom i 2004/563/WE, Euratom ([3])).

([1]) Por. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité" z dnia 31 grudnia 2004 r., „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" z dnia 20 stycznia 2007 r. i „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" z dnia 22 lipca 1959 r.

([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]) Decyzja Komisji 2004/563/WE, Euratom z dnia 7 lipca 2004 r. zmieniająca jej regulamin wewnętrzny (Dz.U. L 251 z 27.7.2004, s. 9).

(8) Przepisy niniejszej decyzji nie naruszają:

a) rozporządzenia (Euratom) nr 3 ([1]);

b) rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([2]);

c) rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([3]);

d) rozporządzenia Rady (EWG, Euratom) nr 354/83 ([4]),

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

PODSTAWOWE ZASADY I MINIMALNE STANDARDY

Artykuł 1

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

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

2) „materiał kryptograficzny" oznacza algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegóły stosowania i związaną z nim dokumentację oraz klucze;

3) „zniesienie klauzuli tajności" oznacza zniesienie wszelkiej klauzuli tajności;

4) „ochrona w głąb" oznacza stosowanie szeregu środków bezpieczeństwa w formie wielu warstw zabezpieczeń;

5) „dokument" oznacza każdą zapisaną informację, niezależnie od jej postaci fizycznej lub cech;

6) „obniżenie klauzuli tajności" oznacza obniżenie poziomu klauzuli tajności;

7) „korzystanie" z EUCI oznacza wszelkie możliwe działania, jakim mogą być poddawane EUCI w całym cyklu ich życia. Pojęcie to obejmuje tworzenie, rejestrowanie, przetwarzanie i przenoszenie EUCI, obniżanie lub znoszenie ich klauzul tajności oraz niszczenie. W odniesieniu do systemów teleinformatycznych (CIS) pojęcie to obejmuje również gromadzenie, wyświetlanie, przesyłanie i przechowywanie EUCI;

8) „posiadacz" oznacza odpowiednio uprawnioną osobę, której potrzeby w ramach ograniczonego dostępu zostały ustalone i w której posiadaniu znajduje się EUCI, w związku z czym odpowiada ona za ochronę przedmiotowych informacji;

9) „przepisy wykonawcze" oznaczają każdy zbiór przepisów lub instrukcji bezpieczeństwa przyjętych zgodnie z rozdziałem 5 decyzji Komisji (UE, Euratom) 2015/443 ([5]);

10) „materiały" oznaczają dowolny nośnik informacji, nośnik danych lub urządzenie bądź sprzęt, wytworzone lub będące w trakcie wytwarzania;

11) „wytwórca" oznacza instytucję, agencję lub organ UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, w ramach właściwości której wytworzono informacje niejawne lub wprowadzono je do struktur UE;

12) „obiekty" oznaczają dowolną nieruchomość lub inną własność i posiadłość Komisji;

([1]) Rozporządzenie (Euratom) nr 3 z dnia 31 lipca 1958 r. w sprawie wykonania art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej (Dz.U. 17 z 6.10.1958, s. 406/58).

([2]) 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).

([3]) 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).

([4]) Rozporządzenie Rady (EWG, Euratom) nr 354/83 z dnia 1 lutego 1983 r. dotyczące udostępnienia do wglądu publicznego historycznych materiałów archiwalnych Europejskiej Wspólnoty Gospodarczej i Europejskiej Wspólnoty Energii Atomowej (Dz.U. L 43 z 15.2.1983, s. 1).

([5]) Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (zob. s. 41 niniejszego Dziennika Urzędowego).

13) „proces zarządzania ryzykiem związanym z bezpieczeństwem" oznacza całość procesu określania, kontrolowania i minimalizacji niepewnych zdarzeń, które mogą wpłynąć na bezpieczeństwo danej organizacji lub każdego używanego przez nią systemu. Obejmuje on wszystkie działania związane z ryzykiem, w tym ocenę, zmniejszanie ryzyka, akceptację i powiadamianie;

14) „regulamin pracowniczy" oznacza Regulamin pracowniczy urzędników Unii Europejskiej i warunki zatrudnienia innych pracowników Unii Europejskiej ustanowiony rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 ([1]);

15) „zagrożenie" oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla organizacji lub systemu przez nią używanego; zagrożenia takie mogą być przypadkowe lub zamierzone (rozmyślne) i obejmują elementy zagrażające, potencjalne cele i metody ataku;

16) „podatność" oznacza każdego rodzaju słaby punkt, który może zostać wykorzystany przez jedno zagrożenie lub większą ich liczbę. Podatność może być zaniechaniem lub może odnosić się do słabego punktu środków kontroli, jeżeli chodzi o ich solidność, wszechstronność lub spójność; może mieć charakter techniczny, proceduralny, fizyczny, organizacyjny lub operacyjny.

Artykuł 2

Przedmiot i zakres

1. W niniejszej decyzji określono podstawowe zasady i minimalne standardy bezpieczeństwa służące ochronie EUCI.

2. Niniejszą decyzję stosuje się do wszystkich departamentów Komisji i do wszystkich obiektów Komisji.

3. Nie naruszając żadnych konkretnych wskazań dotyczących poszczególnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Komisji, pracowników Komisji objętych regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Wspólnot Europejskich, ekspertów krajowych oddelegowanych do Komisji, dostawców usług i ich pracowników, stażystów oraz do wszystkich osób mających dostęp do budynków lub innych aktywów Komisji lub do informacji przetwarzanych przez Komisję.

4. Przepisy niniejszej decyzji nie naruszają decyzji 2002/47/WE, EWWiS, Euratom i decyzji 2004/563/WE, Euratom.

Artykuł 3

Definicja EUCI, klauzule tajności i oznaczenia

1. „Informacje niejawne Unii Europejskiej" (EUCI) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby spowodować szkody różnego stopnia dla interesów Unii Europejskiej lub interesów co najmniej jednego państwa członkowskiego.

2. EUCI otrzymują jedną z następujących klauzul tajności:

a) TRES SECRET UE/EU TOP SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

b) SECRET UE/EU SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

d) RESTREINT UE/EU RESTRICTED: informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego.

3. EUCI opatruje się oznaczeniem klauzuli tajności zgodnie z ust. 2. Można opatrzyć je dodatkowymi oznaczeniami, które nie są oznaczeniami klauzul tajności, natomiast mają wskazywać dziedzinę działalności, do której się odnoszą, wytwórcę, ograniczenie dystrybucji, ograniczenie wykorzystania lub możliwość ujawnienia.

([1]) Rozporządzenie Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiające Regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Wspólnot Europejskich oraz ustanawiające specjalne środki stosowane tymczasowo wobec urzędników Komisji (warunki zatrudnienia innych pracowników) (Dz.U. L 56 z 4.3.1968, s. 1).

Artykuł 4

Zarządzanie klauzulami tajności

1. Każdy członek Komisji lub departamentu Komisji zapewnia, by wytworzonym przez niego EUCI nadawano odpowiednie klauzule tajności, by informacje takie były wyraźnie oznaczone jako EUCI, a także by były objęte danym poziomem klauzuli tajności nie dłużej, niż jest to konieczne.

2. Bez uszczerbku dla przepisów art. 26 poniżej, do obniżenia lub zniesienia klauzuli tajności nadanej EUCI lub do zmiany lub usunięcia oznaczeń klauzuli tajności, o których mowa w art. 3 ust. 2, potrzebna jest uprzednia pisemna zgoda wytwórcy.

3. W stosownych przypadkach przyjmuje się, w myśl art. 60 poniżej, przepisy wykonawcze dotyczące korzystania z EUCI, w tym praktyczny przewodnik nadawania klauzul tajności.

Artykuł 5

Ochrona informacji niejawnych

1. EUCI są chronione zgodnie z niniejszą decyzją i z jej przepisami wykonawczymi.

2. Posiadacz jakiegokolwiek elementu EUCI jest odpowiedzialny za jego ochronę zgodnie z niniejszą decyzją i z jej przepisami wykonawczymi, w myśl zasad określonych w rozdziale 4 poniżej.

3. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci Komisji informacje niejawne opatrzone oznaczeniem krajowej klauzuli tajności, Komisja obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI o równorzędnej klauzuli tajności – zgodnie z tabelą odpowiedników klauzul tajności zamieszczoną w załączniku I.

4. Uzasadnione może być objęcie zagregowanych EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności niż klauzula nadana poszczególnym elementom tego zbioru.

Artykuł 6

Zarządzanie ryzykiem związanym z bezpieczeństwem

1. Środki bezpieczeństwa służące ochronie EUCI na wszystkich etapach ich cyklu życia są proporcjonalne w szczególności do ich klauzuli tajności, formy, ilości informacji lub materiałów, lokalizacji i konstrukcji obiektów, w których się znajdują, oraz oceny niebezpieczeństwa, że w miejscu tym podejmowane będą działania w złych zamiarach lub działalność przestępcza, taka jak działalność szpiegowska, sabotażowa lub terrorystyczna.

2. Plany awaryjne uwzględniają potrzebę ochrony EUCI w sytuacjach nadzwyczajnych, w celu zapobieżenia nieuprawnionemu dostępowi do informacji, ich ujawnieniu lub utracie ich integralności lub dostępności.

3. W planach ciągłości działania wszystkich służb przewidywane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z korzystaniem z EUCI oraz z ich przechowywaniem.

Artykuł 7

Wykonanie niniejszej decyzji

1. W razie potrzeby przyjmuje się, w myśl art. 60 poniżej, przepisy wykonawcze w celu uzupełnienia lub wsparcia niniejszej decyzji.

2. Departamenty Komisji podejmują wszelkie niezbędne działania leżące w zakresie ich odpowiedzialności w celu zapewnienia stosowania niniejszej decyzji i odpowiednich przepisów wykonawczych przy korzystaniu z EUCI lub jakichkolwiek innych informacji niejawnych bądź ich przechowywaniu.

3. Środki bezpieczeństwa stosowane podczas wykonywania niniejszej decyzji są zgodne z zasadami dotyczącymi bezpieczeństwa w Komisji określonymi w art. 3 decyzji (UE, Euratom) 2015/443.

4. Dyrektor generalny ds. zasobów ludzkich i bezpieczeństwa powołuje organ ds. bezpieczeństwa Komisji w ramach Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa. Na podstawie niniejszej decyzji i jej przepisów wykonawczych organowi ds. bezpieczeństwa Komisji powierza się jego obowiązki.

5. W ramach każdego departamentu Komisji lokalnemu pełnomocnikowi ochrony (LSO), o którym mowa w art. 20 decyzji (UE, Euratom) 2015/443, zgodnie z niniejszą decyzją powierza się następujące ogólne obowiązki dotyczące ochrony EUCI wykonywane w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa:

a) obsługa wniosków w sprawie upoważnień w zakresie bezpieczeństwa wydawanych pracownikom;

b) wkład w szkolenia i instrukcje w zakresie bezpieczeństwa;

c) nadzór nad urzędnikiem kontroli kancelarii departamentu;

d) zgłaszanie naruszenia i narażenia na szwank bezpieczeństwa EUCI;

e) przechowywanie zapasowych kluczy i pisemny rejestr kodów;

f) realizacja innych zadań związanych z ochroną EUCI lub określonych w ramach przepisów wykonawczych.

Artykuł 8

Naruszenie zasad bezpieczeństwa i narażenie na szwank bezpieczeństwa EUCI

1. Naruszenie zasad bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania, sprzecznego z przepisami bezpieczeństwa określonymi w niniejszej decyzji i jej przepisach wykonawczych.

2. Narażenie na szwank bezpieczeństwa EUCI ma miejsce, gdy w wyniku naruszenia zasad bezpieczeństwa takie informacje w całości lub w części zostają ujawnione osobom nieupoważnionym.

3. O każdym podejrzeniu lub przypadku naruszenia zasad bezpieczeństwa powiadamia się niezwłocznie organ ds. bezpieczeństwa Komisji.

4. W przypadkach, gdy wiadomo lub istnieją racjonalne podstawy do podejrzeń, że bezpieczeństwo EUCI zostało narażone na szwank lub że informacje takie zostały utracone, zgodnie z art. 13 decyzji (UE, Euratom) 2015/443 przeprowadza się dochodzenie w sprawie bezpieczeństwa.

5. Podejmuje się wszelkie stosowne środki w celu:

a) poinformowania wytwórcy informacji;

b) zapewnienia zbadania tego przypadku przez pracowników niezwiązanych bezpośrednio z przedmiotowym naruszeniem w celu ustalenia faktów;

c) oceny potencjalnych szkód, jakie poniosły interesy Unii lub państwa członkowskie;

d) podjęcia właściwych środków, aby zapobiec powtórzeniu się podobnego przypadku oraz

e) powiadomienia właściwych organów o podjętych działaniach.

6. Każda osoba odpowiedzialna za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji może podlegać postępowaniu dyscyplinarnemu zgodnie z regulaminem pracowniczym. Każda osoba odpowiedzialna za narażenie na szwank bezpieczeństwa EUCI lub za ich utratę podlega postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

ROZDZIAŁ 2

BEZPIECZEŃSTWO OSOBOWE

Artykuł 9

Definicje

Do celów niniejszego rozdziału stosuje się poniższe definicje:

1) „upoważnienie do dostępu do EUCI" oznacza decyzję organu ds. bezpieczeństwa Komisji podjętą na podstawie zapewnienia udzielonego przez właściwy organ państwa członkowskiego, że urzędnik Komisji, inny pracownik lub oddelegowany ekspert krajowy – o ile ustalono jego potrzeby dostępu w ramach zasady ograniczonego dostępu i został on odpowiednio poinstruowany o zakresie swoich obowiązków – może uzyskać dostęp do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty; o osobie takiej mówi się, że jest „upoważniona w zakresie bezpieczeństwa";

2) „upoważnienie w zakresie bezpieczeństwa osobowego" oznacza stosowanie środków zapewniających, by dostęp do EUCI był przyznawany tylko osobom, które:

   a) muszą mieć dostęp w ramach zasady ograniczonego dostępu;

   b) w stosownych przypadkach zostały upoważnione w zakresie bezpieczeństwa na odpowiednim poziomie oraz

   c) zostały poinstruowane o swoich obowiązkach;

3) „poświadczenie bezpieczeństwa osobowego" (PBO) oznacza oświadczenie właściwego organu państwa członkowskiego, wydawane po zakończeniu postępowania sprawdzającego prowadzonego przez właściwe organy państwa członkowskiego; stanowi ono potwierdzenie, że dana osoba – o ile ustalono potrzeby dostępu tej osoby w ramach zasady ograniczonego dostępu i została ona odpowiednio poinstruowana o zakresie swoich obowiązków – może uzyskać dostęp do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty;

4) „zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" (ZPBO) oznacza zaświadczenie wydane przez właściwy organ, potwierdzające, że dana osoba posiada ważne poświadczenie bezpieczeństwa lub upoważnienie w zakresie bezpieczeństwa wydane przez organ ds. bezpieczeństwa Komisji oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższym), okresie ważności odpowiedniego poświadczenia bezpieczeństwa lub upoważnienia w zakresie bezpieczeństwa oraz dacie ważności samego zaświadczenia;

5) „postępowanie sprawdzające" oznacza procedury sprawdzające przeprowadzane przez właściwy organ państwa członkowskiego zgodnie z jego krajowymi przepisami ustawowymi i wykonawczymi w celu uzyskania pewności, że nie istnieją żadne znane niekorzystne okoliczności, które mogłyby stanowić przeszkodę w wydaniu danej osobie poświadczenia bezpieczeństwa do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego).

Artykuł 10

Podstawowe zasady

1. Danej osobie można udzielić dostępu do EUCI wyłącznie po tym, jak:

1) określono jej potrzeby w ramach zasady ograniczonego dostępu;

2) została ona poinstruowana o przepisach bezpieczeństwa służących ochronie EUCI oraz odnośnych standardach i wytycznych dotyczących bezpieczeństwa i potwierdziła, że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji;

3) w przypadku informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą – otrzymała upoważnienie w zakresie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez nią funkcje przyznano jej inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

2. Wszystkie osoby, których obowiązki mogą wymagać dostępu do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, otrzymują przed uzyskaniem dostępu do takich EUCI upoważnienie w zakresie bezpieczeństwa do odpowiedniego poziomu. Dana osoba wyraża na piśmie zgodę na poddanie się procedurze sprawdzającej w zakresie poświadczenia bezpieczeństwa osobowego. Jeżeli dana osoba tego nie uczyni, nie może objąć stanowiska, pełnić funkcji lub wykonywać zadania, które związane są z dostępem do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą.

3. Procedury sprawdzające w zakresie poświadczenia bezpieczeństwa osobowego mają na celu stwierdzenie, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnić do dostępu do EUCI.

4. Organ państwa członkowskiego określa lojalność, wiarygodność i rzetelność, danej osoby, przeprowadzając właściwe postępowanie sprawdzające zgodnie ze swoimi krajowymi przepisami ustawowymi i wykonawczymi i ustalając, czy może zostać ona upoważniona do dostępu do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą.

5. Organ ds. bezpieczeństwa Komisji ponosi wyłączną odpowiedzialność za utrzymywanie kontaktów z krajowymi władzami bezpieczeństwa („KWB") lub innymi właściwymi organami krajowymi w zakresie wszystkich kwestii dotyczących poświadczenia bezpieczeństwa. Wszelkie kontakty między służbami Komisji, jej pracownikami, KWB i innymi właściwymi organami krajowymi odbywają się za pośrednictwem organu ds. bezpieczeństwa Komisji.

Artykuł 11

Procedura wydawania upoważnień w zakresie bezpieczeństwa

1. Każdy dyrektor generalny lub szef służby Komisji określa w swoim departamencie stanowiska, na których zatrudnione osoby muszą mieć dostęp do informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, w związku z czym muszą one zostać odpowiednio sprawdzone pod kątem bezpieczeństwa.

2. Niezwłocznie po uzyskaniu informacji, że dana osoba zostanie powołana na stanowisko wymagające dostępu do informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, lokalny pełnomocnik ochrony danego departamentu Komisji informuje organ ds. bezpieczeństwa Komisji, który przekazuje danej osobie kwestionariusz postępowania sprawdzającego wydany przez KWB państwa członkowskiego, którego obywatelstwo posiada osoba mianowana na pracownika instytucji Unii Europejskiej. Dana osoba wyraża na piśmie zgodę na poddanie się procedurze sprawdzającej w zakresie poświadczenia bezpieczeństwa i zwraca wypełniony kwestionariusz organowi ds. bezpieczeństwa Komisji w jak najkrótszym terminie.

3. Organ ds. bezpieczeństwa Komisji przekazuje wypełniony kwestionariusz postępowania sprawdzającego do KWB państwa członkowskiego, którego obywatelstwo posiada osoba mianowana na pracownika instytucji Unii Europejskiej, z wnioskiem o przeprowadzenie postępowania sprawdzającego do poziomu EUCI, do którego dostęp będzie w przypadku tej osoby niezbędny.

4. Jeżeli organ ds. bezpieczeństwa Komisji posiada informację istotną w odniesieniu do postępowania sprawdzającego prowadzonego wobec osoby, która złożyła wniosek o poświadczenie bezpieczeństwa, organ ds. bezpieczeństwa Komisji powiadamia o tym właściwą KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.

5. Po zakończeniu postępowania sprawdzającego, a także jak najwcześniej po powiadomieniu odpowiedniego KWB o ogólnej ocenie wniosków z postępowania sprawdzającego, organ ds. bezpieczeństwa Komisji:

a) jeżeli w wyniku postępowania sprawdzającego uzyskuje się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważać lojalność, wiarygodność i rzetelność danej osoby – organ może przyznać upoważnienie do dostępu do EUCI danej osobie oraz upoważnić ją do dostępu do EUCI do odpowiedniego poziomu i do określonej przez organ daty, jednak nie dłużej niż na okres 5 lat;

b) jeżeli w wyniku postępowania sprawdzającego nie uzyskuje się takiej pewności – zgodnie z odpowiednimi zasadami i przepisami wykonawczymi organ powiadamia o tym fakcie daną osobę, która może zwrócić się do organu ds. bezpieczeństwa Komisji z prośbą o wysłuchanie; ten ostatni może z kolei zwrócić się do właściwego KWB z prośbą o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik postępowania sprawdzającego zostanie potwierdzony, nie wydaje się upoważnienia do dostępu do EUCI.

6. Postępowanie sprawdzające oraz jego wyniki podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu ds. bezpieczeństwa Komisji podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym.

7. Komisja akceptuje upoważnienie do dostępu do EUCI wydane przez każdą inną instytucję, organ lub jednostkę organizacyjną Unii, o ile pozostaje ono ważne. Upoważnienia dotyczą każdego zadania powierzonego danej osobie w obrębie Komisji. Instytucja, organ lub jednostka organizacyjna Unii, w której dana osoba zostaje zatrudniona, poinformuje odpowiednią KWB o tej zmianie pracodawcy.

8. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu ds. bezpieczeństwa Komisji o wyniku postępowania sprawdzającego lub jeżeli w pełnieniu obowiązków przez daną osobę występuje 12-miesięczna przerwa, w czasie której osoba ta nie jest zatrudniona przez Komisję lub inną instytucję, organ lub jednostkę organizacyjną Unii, ani na żadnym stanowisku w administracji krajowej państwa członkowskiego, organ ds. bezpieczeństwa Komisji kieruje sprawę do odpowiedniej KWB w celu potwierdzenia, czy poświadczenie bezpieczeństwa nadal pozostaje ważne i właściwe.

9. Jeżeli organ bezpieczeństwa Komisji znajdzie się w posiadaniu informacji o zagrożeniu dla zasad bezpieczeństwa ze strony osoby, która posiada ważne upoważnienie w zakresie bezpieczeństwa, organ ds. bezpieczeństwa Komisji powiadamia o tym właściwą KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.

10. Jeżeli KWB powiadomi organ ds. bezpieczeństwa Komisji o utracie pewności uzyskanej zgodnie z ust. 5 lit. a) w odniesieniu do osoby posiadającej ważne upoważnienie do dostępu do EUCI, organ bezpieczeństwa Komisji może zwrócić się do KWB o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone przez odpowiednią KWB, upoważnienie w zakresie bezpieczeństwa zostaje cofnięte, a osobie takiej odbiera się prawo dostępu do EUCI i odsuwa się ją od stanowisk, na których taki dostęp jest możliwy lub na których osoba ta mogłaby zagrażać bezpieczeństwu.

11. O każdej decyzji w sprawie cofnięcia lub zawieszenia upoważnienia do dostępu do EUCI przyznanego każdej osobie objętej zakresem stosowania niniejszej decyzji i w stosownych przypadkach o przyczynach tego cofnięcia lub zawieszenia powiadamia się daną osobę, która może zwrócić się do organu ds. bezpieczeństwa Komisji z prośbą o wysłuchanie. Informacje przedstawione przez KWB podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim. Decyzje podjęte w tym zakresie przez organ ds. bezpieczeństwa Komisji podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym.

12. Departamenty Komisji upewniają się, czy przed podjęciem się swojego zadania eksperci krajowi oddelegowani do nich na stanowisko wymagające upoważnienia w zakresie bezpieczeństwa do dostępu do EUCI przedstawiają organowi ds. bezpieczeństwa Komisji ważne poświadczenie bezpieczeństwa lub zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego („ZPBO") zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; organ ds. bezpieczeństwa Komisji na tej podstawie przyzna upoważnienie bezpieczeństwa do dostępu do EUCI do poziomu odpowiadającego poziomowi określonemu w krajowym poświadczeniu bezpieczeństwa nie dłużej niż na okres wykonywania ich zadań.

Dostęp do EUCI osób odpowiednio upoważnionych ze względu na pełnione przez nich funkcje

13. Członkowie Komisji, którzy posiadają dostęp do EUCI ze względu na pełnione przez nich funkcje na podstawie Traktatu, są informowani o spoczywających na nich obowiązkach dotyczących bezpieczeństwa w odniesieniu do ochrony EUCI.

Rejestry poświadczeń bezpieczeństwa i upoważnień w zakresie bezpieczeństwa

14. Zgodnie z niniejszą decyzją rejestry poświadczeń bezpieczeństwa i upoważnień udzielonych w zakresie dostępu do EUCI prowadzone są przez organ ds. bezpieczeństwa Komisji. Rejestry te zawierają co najmniej poziom klauzuli tajności EUCI, do których dana osoba może mieć dostęp, datę przyznania poświadczenia bezpieczeństwa i okres jego ważności.

15. Organ ds. bezpieczeństwa Komisji może wydać ZPBO określające poziom klauzuli tajności EUCI, do których danej osobie można zapewnić dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okres ważności odpowiedniego upoważnienia do dostępu do EUCI oraz datę ważności samego zaświadczenia.

Przedłużanie ważności upoważnień w zakresie bezpieczeństwa

16. Po wydaniu pierwszego upoważnienia w zakresie bezpieczeństwa oraz pod warunkiem że w zatrudnieniu danej osoby w Komisji Europejskiej lub innej instytucji, organie lub jednostce organizacyjnej Unii nie wystąpiły przerwy, a dostęp do EUCI jest jej stale potrzebny, przedłużenie ważności upoważnienia w zakresie bezpieczeństwa do dostępu do EUCI rozpatrywane jest zasadniczo w odstępach czasu nieprzekraczających pięciu lat, licząc od daty powiadomienia o wyniku ostatniego postępowania sprawdzającego, na podstawie którego zostało wydane to poświadczenie.

17. Organ ds. bezpieczeństwa Komisji może przedłużyć ważność obowiązującego upoważnienia w zakresie bezpieczeństwa na okres nieprzekraczający 12 miesięcy, jeżeli odpowiednia KWB lub inny właściwy organ krajowy nie przekazał żadnych niekorzystnych informacji w okresie dwóch miesięcy od daty przekazania wniosku o przedłużenie ważności i właściwego kwestionariusza bezpieczeństwa. Jeżeli pod koniec tego 12-miesięcznego okresu odpowiednia KWB lub inny właściwy organ krajowy nie przekazał organowi ds. bezpieczeństwa Komisji swojej opinii, danej osobie przydziela się obowiązki, które nie wymagają posiadania upoważnienia w zakresie bezpieczeństwa.

Artykuł 12

Instrukcje dotyczące upoważnień w zakresie bezpieczeństwa

1. Po uczestnictwie w instruktażu dotyczącym upoważnień w zakresie bezpieczeństwa zorganizowanym przez organ ds. bezpieczeństwa Komisji wszystkie osoby, które uzyskały upoważnienie w zakresie bezpieczeństwa, oświadczają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank bezpieczeństwa EUCI. Wykaz takich pisemnych oświadczeń przechowywany jest przez organ ds. bezpieczeństwa Komisji.

2. Wszystkie osoby, które zostały upoważnione do dostępu do EUCI lub muszą korzystać z tych informacji, są na początku powiadamiane o zagrożeniach bezpieczeństwa, a następnie regularnie informowane o tych zagrożeniach; osoby te muszą bezzwłocznie zgłaszać organowi ds. bezpieczeństwa Komisji wszelkie zdarzenia lub wszelkie działania, które uznają za podejrzane lub nietypowe.

3. Wszystkie osoby, które przestają wykonywać obowiązki wymagające dostępu do EUCI, powiadamiane są o obowiązku kontynuowania ochrony EUCI, a w stosownych przypadkach potwierdzają świadomość tego obowiązku na piśmie.

Artykuł 13

Tymczasowe upoważnienia w zakresie bezpieczeństwa

1. W wyjątkowych okolicznościach, jeżeli jest to należycie uzasadnione interesami jednostki organizacyjnej, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ ds. bezpieczeństwa Komisji może, po konsultacji z KWB państwa członkowskiego, którego obywatelem jest dana osoba, oraz pod warunkiem że wynik wstępnego sprawdzenia nie wykazał niekorzystnych informacji, wydać danym osobom tymczasowe uprawnienie do dostępu do EUCI, by mogły wykonać określone zadania, nie naruszając przepisów dotyczących przedłużenia ważności poświadczeń bezpieczeństwa. Przedmiotowe tymczasowe uprawnienia do dostępu do EUCI zachowują ważność przez jeden okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji niejawnych z klauzulą tajności TRES SECRET UE/EU TOP SECRET.

2. Po instruktażu przeprowadzonym zgodnie z art. 12 ust. 1 wszystkie osoby, którym przyznano tymczasowe upoważnienie, oświadczają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank bezpieczeństwa EUCI. Wykaz takich pisemnych oświadczeń przechowywany jest przez organ ds. bezpieczeństwa Komisji.

Artykuł 14

Uczestnictwo w niejawnych posiedzeniach organizowanych przez Komisję

1. Departamenty Komisji odpowiedzialne za organizację posiedzeń, na których omawiane są informacje niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, powiadamiają organ ds. bezpieczeństwa Komisji o dacie, godzinie, miejscu obrad i uczestnikach takich posiedzeń; dokonują tego z dużym wyprzedzeniem i za pośrednictwem swojego lokalnego pełnomocnika ochrony lub organizatora posiedzenia.

2. Z zastrzeżeniem przepisów art. 11 ust. 13 osoby wyznaczone do udziału w posiedzeniach zorganizowanych przez Komisję, podczas których omawiane są informacje niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, mogą brać w nich udział tylko po potwierdzeniu statusu ich poświadczenia bezpieczeństwa lub upoważnienia w zakresie bezpieczeństwa. W przedmiotowych niejawnych posiedzeniach nie mogą uczestniczyć osoby, które nie przedłożyły organowi ds. bezpieczeństwa Komisji ZPBO lub innego dowodu posiadania przez nie poświadczenia bezpieczeństwa, lub członkowie Komisji, którzy nie posiadają upoważnienia w zakresie bezpieczeństwa.

3. Przed zorganizowaniem niejawnego posiedzenia odpowiedzialny za nie organizator lub lokalny pełnomocnik ochrony departamentu Komisji organizującego posiedzenie zwraca się do zewnętrznych uczestników z prośbą o dostarczenie organowi ds. bezpieczeństwa Komisji ZPBO lub innego dowodu posiadania poświadczenia bezpieczeństwa. Organ ds. bezpieczeństwa Komisji powiadamia lokalnego pełnomocnika ochrony lub organizatora posiedzeń o otrzymaniu ZPBO lub innych dowodów posiadania przez uczestników PBO. W stosownych przypadkach można zastosować skonsolidowany wykaz nazwisk zawierający odpowiednie dowody posiadania poświadczenia bezpieczeństwa.

4. Jeżeli organ ds. bezpieczeństwa Komisji zostanie poinformowany przez właściwe organy o cofnięciu poświadczenia bezpieczeństwa osobowego w przypadku osoby, której obowiązki wymagają udziału w posiedzeniach zorganizowanych przez Komisję, organ ds. bezpieczeństwa Komisji powiadamia lokalnego pełnomocnika ochrony departamentu Komisji odpowiedzialnego za organizację posiedzenia.

Artykuł 15

Potencjalny dostęp do EUCI

Kurierzy, strażnicy i eskorta zostają upoważnieni w zakresie bezpieczeństwa do celów dostępu do informacji z odpowiednią klauzulą tajności lub w inny sposób odpowiednio sprawdzeni zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, poinstruowani o procedurach bezpieczeństwa w zakresie ochrony EUCI oraz pouczeni o obowiązku ochrony informacji, które im powierzono.

ROZDZIAŁ 3

BEZPIECZEŃSTWO FIZYCZNE MAJĄCE NA CELU OCHRONĘ INFORMACJI NIEJAWNYCH

Artykuł 16

Podstawowe zasady

1. Środki bezpieczeństwa fizycznego mają na celu zapobiegać wtargnięciu osoby nieupoważnionej w sposób niezauważony lub z użyciem siły, powstrzymanie od podjęcia nieuprawnionych działań, udaremnienie ich i wykrycie oraz umożliwienie podziału pracowników pod względem potrzeby dostępu do EUCI zgodnie z zasadą ograniczonego dostępu. Środki te określane są na podstawie procesu zarządzania ryzykiem zgodnie z niniejszą decyzją i z jej przepisami wykonawczymi.

2. W szczególności środki bezpieczeństwa fizycznego mają na celu zapobiegać nieuprawnionemu dostępowi do EUCI dzięki:

a) zapewnieniu właściwego postępowania z EUCI i ich przechowywania;

b) umożliwieniu podziału pracowników pod względem potrzeby dostępu do EUCI zgodnie z zasadą ograniczonego dostępu i, w stosownych przypadkach, pod względem ich upoważnienia w zakresie bezpieczeństwa;

c) powstrzymywaniu nieuprawnionych działań, ich udaremnianiu i wykrywaniu; oraz

d) uniemożliwieniu lub opóźnieniu wtargnięcia osób nieupoważnionych w sposób niezauważony lub z użyciem siły.

3. Środki bezpieczeństwa fizycznego wprowadza się we wszystkich obiektach, budynkach, biurach, pomieszczeniach i innych strefach, w których są wykorzystywane lub przechowywane EUCI, w tym w strefach, w których znajdują się systemy teleinformatyczne określone w rozdziale 5.

4. Zgodnie z niniejszym rozdziałem strefy, w których przechowywane są EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, ustanawia się jako strefy bezpieczeństwa; strefy takie zatwierdza organ ds. akredytacji bezpieczeństwa Komisji Europejskiej.

5. Do ochrony EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą stosuje się wyłącznie sprzęt lub urządzenia zatwierdzone przez organ ds. bezpieczeństwa Komisji.

Artykuł 17

Wymogi i środki w zakresie bezpieczeństwa fizycznego

1. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez organ ds. bezpieczeństwa Komisji, w stosownych przypadkach po konsultacji z innymi departamentami Komisji, innymi instytucjami, agencjami lub organami UE lub właściwymi organami w państwach członkowskich. Komisja stosuje w swoich obiektach proces zarządzania ryzykiem służący ochronie EUCI, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. Proces zarządzania ryzykiem uwzględnia wszelkie istotne czynniki, a w szczególności:

a) klauzulę tajności EUCI;

b) postać i ilość EUCI z uwzględnieniem faktu, że duża ilość EUCI lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochronnych;

c) otoczenie i strukturę budynków lub stref, w których znajdują się EUCI; oraz

d) szacowane zagrożenie ze strony służb wywiadowczych, których celem jest Unia, jej instytucje, organy lub agencje, lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.

2. Stosując koncepcję ochrony w głąb, organ ds. bezpieczeństwa Komisji określa właściwą kombinację środków bezpieczeństwa fizycznego, które należy wdrożyć. W tym celu organ ds. bezpieczeństwa Komisji opracowuje minimalne normy, standardy i kryteria określone w przepisach wykonawczych.

3. Organ ds. bezpieczeństwa Komisji jest uprawniony do przeszukiwania osób wchodzących i wychodzących w formie środka odstraszającego przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z obiektów lub budynków.

4. Jeżeli istnieje ryzyko podglądu EUCI, także przypadkowego, odpowiednie departamenty Komisji podejmują stosowne środki określone przez organ ds. bezpieczeństwa Komisji w celu zlikwidowania takiego ryzyka.

5. W przypadku nowych obiektów wymogi dotyczące bezpieczeństwa fizycznego i specyfikacje dotyczące ich stosowania zostają określone w porozumieniu z organem ds. bezpieczeństwa Komisji na etapie planowania i projektowania tych obiektów. W przypadku obiektów już istniejących wymogi dotyczące bezpieczeństwa fizycznego stosowane są zgodnie z minimalnymi normami, standardami i kryteriami określonymi w przepisach wykonawczych.

Artykuł 18

Sprzęt służący do fizycznej ochrony EUCI

1. Ustanawia się dwa rodzaje stref chronionych fizycznie służących fizycznej ochronie EUCI:

a) strefy administracyjne; oraz

b) strefy bezpieczeństwa (w tym strefy technicznie zabezpieczone).

2. Organ Komisji ds. akredytacji bezpieczeństwa stwierdza, czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną, strefę bezpieczeństwa lub strefę technicznie zabezpieczoną.

3. W przypadku stref administracyjnych:

a) wyraźnie określa się granicę umożliwiającą kontrolę osób i, jeżeli to możliwe, pojazdów;

b) dostęp bez eskorty umożliwia się tylko osobom, które są odpowiednio upoważnione przez organ ds. bezpieczeństwa Komisji lub każdy inny właściwy organ; oraz

c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.

4. W przypadku stref bezpieczeństwa:

a) wyraźnie określa się i chroni granicę, na której wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób;

b) dostęp bez eskorty umożliwia się tylko osobom odpowiednio sprawdzonym w zakresie poświadczenia bezpieczeństwa i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z ich potrzebą dostępu w ramach zasady ograniczonego dostępu;

c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.

5. Jeżeli wejście do strefy bezpieczeństwa jest w praktyce równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie, zastosowanie mają następujące wymogi dodatkowe:

a) wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie;

b) wszystkie osoby wchodzące muszą posiadać specjalne upoważnienie do wejścia do tej strefy, przez cały czas towarzyszy im eskorta, a także muszą być odpowiednio sprawdzone w zakresie poświadczenia bezpieczeństwa, chyba że podjęte zostały kroki służące zapewnieniu, by dostęp do EUCI był niemożliwy.

6. Strefy bezpieczeństwa chronione przed podsłuchem uznawane są za strefy technicznie zabezpieczone. Zastosowanie mają następujące dodatkowe wymogi:

a) strefy takie wyposażone są w system sygnalizacji włamania i napadu (SSWiN), są zamknięte na klucz, gdy nikt w nich nie przebywa, i pilnowane, gdy ktoś w nich przebywa. Wszystkimi kluczami zarządza się zgodnie z art. 20;

b) wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli;

c) strefy takie podlegają regularnym inspekcjom fizycznym lub technicznym przeprowadzanym przez organ ds. bezpieczeństwa Komisji. Inspekcje takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce; oraz

d) w strefach takich nie mogą się znajdować zainstalowane bez upoważnienia linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.

7. Niezależnie od ust. 6 lit. d), zanim urządzenia komunikacyjne i sprzęt elektryczny lub elektroniczny zostaną użyte w strefach, w których odbywają się posiedzenia lub prowadzone są prace związane z wykorzystaniem informacji niejawnych z klauzulą tajności SECRET UE/EU SECRET i wyższą, a także jeżeli ocenia się, że istnieje wysokie zagrożenie dla EUCI, przedmiotowe urządzenia i sprzęt zostają najpierw sprawdzone przez organ ds. bezpieczeństwa Komisji, aby żadne zrozumiałe informacje nie zostały nieumyślnie lub nielegalnie przesłane przez przedmiotowy sprzęt poza granicę strefy bezpieczeństwa.

8. Strefy bezpieczeństwa, w których nie pracują w systemie całodobowym pracownicy pełniący dyżur, są w odpowiednich przypadkach poddawane inspekcji na koniec normalnych godzin pracy i w przypadkowych odstępach czasu poza tymi godzinami, chyba że znajdują się tam SSWiN.

9. Strefy bezpieczeństwa oraz strefy technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu.

10. Lokalny pełnomocnik ochrony odpowiedniego departamentu Komisji opracowuje procedury bezpiecznej eksploatacji systemu (SecOP) w odniesieniu do każdej strefy bezpieczeństwa podlegającej jego nadzorowi, określając (zgodnie z przepisami niniejszej decyzji i jej przepisami wykonawczymi):

a) poziom klauzuli tajności EUCI, z których można korzystać i które można przechowywać w tej strefie;

b) środki nadzoru i środki ochronne, które należy stosować;

c) osoby upoważnione do wejścia do strefy bez eskorty ze względu ich potrzebę dostępu i posiadane upoważnienia w zakresie bezpieczeństwa;

d) w odpowiednich przypadkach procedury dotyczące eskort lub ochrony EUCI, jeżeli zezwala się na wejście do strefy innym osobom;

e) wszelkie inne odpowiednie środki i procedury.

11. W obrębie stref bezpieczeństwa są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i wyposażone w zamek drzwi zatwierdzane są przez organ ds. bezpieczeństwa Komisji i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI z taką samą klauzulą tajności.

Artykuł 19

Fizyczne środki ochronne dotyczące korzystania z EUCI i ich przechowywania

1. Z EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED można korzystać:

a) w strefie bezpieczeństwa;

b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych lub

c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz przenosi EUCI zgodnie z art. 31 i zobowiązał się do zastosowania środków zastępczych określonych w ramach środków wykonawczych w celu zapewnienia ochrony EUCI przed dostępem osób nieupoważnionych.

2. EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED przechowywane są w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. Mogą być one tymczasowo przechowywane poza strefą administracyjną lub strefą bezpieczeństwa, pod warunkiem że posiadacz zobowiązał się do zastosowania środków zastępczych określonych w przepisach wykonawczych.

3. Z EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET można korzystać:

a) w strefie bezpieczeństwa;

b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych lub

c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz:

(i) zobowiązał się do zastosowania środków zastępczych określonych w przepisach wykonawczych w celu zapewnienia ochrony EUCI przed dostępem osób nieupoważnionych;

(ii) przechowuje EUCI przez cały czas pod swoją osobistą kontrolą; oraz

(iii) w przypadku dokumentów w formie papierowej – powiadomił o tym fakcie właściwą kancelarię tajną.

4. EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są w strefie bezpieczeństwa w zabezpieczonej szafie lub wzmocnionym pomieszczeniu.

5. Z EUCI z klauzulą tajności TRES SECRET UE/EU TOP SECRET korzysta się w strefie bezpieczeństwa, ustanowionej i prowadzonej przez organ ds. bezpieczeństwa Komisji, i akredytowanej na tym poziomie tajności przez organ Komisji ds. akredytacji bezpieczeństwa.

6. EUCI z klauzulą tajności TRES SECRET UE/EU TOP SECRET przechowuje się w strefie bezpieczeństwa akredytowanej na tym poziomie tajności przez organ Komisji ds. akredytacji bezpieczeństwa, pod jednym z poniższych warunków:

a) są one przechowywane w zabezpieczonej szafie zgodnie z przepisami art. 18, przy czym zastosowany jest co najmniej jeden z następujących dodatkowych czynników kontrolnych:

1) stała ochrona lub kontrola przez posiadających poświadczenie bezpieczeństwa pracowników ochrony lub pracowników pełniących dyżur;

2) zatwierdzony SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo;

lub

b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo.

Artykuł 20

Zarządzanie kluczami i kodami wykorzystywanymi do ochrony EUCI

1. Zgodnie z art. 60 poniżej procedury zarządzania kluczami i kodami do biur, pomieszczeń, wzmocnionych pomieszczeń i zabezpieczonych szaf określa się w przepisach wykonawczych. Procedury te służą ochronie przed nieuprawnionym dostępem do informacji.

2. Kody zostają powierzone do zapamiętania jak najmniejszej liczbie osób, dla których znajomość tych kodów jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, zostają zmienione:

a) w przypadku otrzymania nowej szafy;

b) przy każdej zmianie pracowników znających kod;

c) każdorazowo gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji;

d) gdy zamek poddano konserwacji lub naprawie; oraz

e) nie rzadziej niż co 12 miesięcy.

ROZDZIAŁ 4

ZARZĄDZANIE INFORMACJAMI NIEJAWNYMI UE

Artykuł 21

Podstawowe zasady

1. Wszystkimi dokumentami zawierającymi EUCI należy zarządzać zgodnie z polityką Komisji dotyczącą zarządzania dokumentami i w związku z tym należy je rejestrować, wypełniać, przechowywać i na koniec usuwać, wyrywkowo kontrolować lub przekazywać do archiwów historycznych, zgodnie ze wspólnym wykazem zatrzymywanych danych na poziomie Komisji w odniesieniu do akt Komisji Europejskiej.

2. Informacje niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Informacje niejawne z klauzulą tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.

3. W obrębie Komisji ustanawia się system kancelarii tajnych UE, zgodnie z przepisami art. 27.

4. Departamenty Komisji i obiekty, w których korzysta się z EUCI lub je przechowuje, poddawane są regularnym inspekcjom prowadzonym przez organ ds. bezpieczeństwa Komisji.

5. Poza strefami chronionymi fizycznie EUCI są przekazywane między jednostkami organizacyjnymi i obiektami w sposób następujący:

a) co do zasady EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z rozdziałem 5;

b) jeżeli nie stosuje się sposobu, o którym mowa w lit. a), EUCI są przekazywane:

   (i) za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z rozdziałem 5; albo

   (ii) we wszystkich innych przypadkach – zgodnie z przepisami wykonawczymi.

Artykuł 22

Klauzule tajności i oznaczenia

1. Jeżeli należy chronić poufność informacji, nadaje się im klauzulę tajności, w myśl art. 3 ust. 1.

2. Jak stanowią odpowiednie przepisy wykonawcze, normy i wytyczne dotyczące nadawania klauzul, za określenie poziomu klauzuli tajności i za początkową dystrybucję informacji odpowiada wytwórca EUCI.

3. Poziom klauzuli tajności EUCI określa się zgodnie z art. 3 ust. 2 i odpowiednimi przepisami wykonawczymi.

4. Klauzulę tajności wskazuje się wyraźnie i poprawnie, niezależnie od tego, czy EUCI występują w pisemnej, ustnej, elektronicznej lub jakiejkolwiek innej formie.

5. Poszczególne części danego dokumentu (np. strony, ustępy, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia) mogą wymagać nadania różnych klauzul tajności i stosowanego oznaczenia, także wtedy, gdy są przechowywane w formie elektronicznej.

6. Ogólna klauzula tajności dokumentu lub pliku jest co najmniej tak wysoka jak klauzula tajności tej części dokumentu, która została oznaczona najwyższą klauzulą tajności. W przypadku zebrania informacji pochodzących z różnych źródeł sprawdza się ostateczną wersję dokumentu w celu określenia jego ogólnej klauzuli tajności, gdyż może istnieć konieczność nadania mu klauzuli tajności wyższej niż klauzule jego poszczególnych części.

7. W stopniu, w jakim jest to możliwe, dokumenty, których częściom nadaje się różne klauzule tajności, są sporządzane w taki sposób, aby części oznaczone różnymi klauzulami można było łatwo zidentyfikować i w razie potrzeby oddzielić.

8. Klauzula tajności pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula tajności nadana załącznikom. Wytwórca wyraźnie wskazuje, jaki poziom klauzuli tajności ma być nadany takiemu pismu lub nocie po ich odłączeniu od załączników, stosując w tym celu odpowiednie oznaczenie, np.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez załącznika(-ów) RESTREINT UE/EU RESTRICTED

Artykuł 23

Oznaczenia

W uzupełnieniu klauzuli tajności, określonej w art. 3 ust. 2, EUCI można opatrzyć dodatkowymi oznaczeniami, do których należą:

a) dane identyfikujące wytwórcę;

b) wszelkie oznaczenia zastrzegające, kody słowne lub akronimy określające obszar działalności, do którego odnosi się dany dokument, szczególny sposób dystrybucji dokumentu zgodnie z zasadą ograniczonego dostępu lub ograniczenia w zakresie wykorzystania;

c) oznaczenia dotyczące możliwości udostępnienia;

d) w stosownych przypadkach data lub konkretne wydarzenie, po których klauzula tajności może zostać obniżona lub zniesiona.

Artykuł 24

Skrócone oznaczenia klauzul tajności

1. W celu nadania poziomu klauzuli tajności pojedynczym ustępom tekstu można stosować standardowe skrócone oznaczenia klauzul tajności. Skróty nie zastępują pełnych nazw klauzul tajności.

2. W celu wskazania poziomu klauzuli tajności sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach niejawnych UE można stosować następujące standardowe skróty:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET S-UE/EU-S	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Artykuł 25

Wytwarzanie EUCI

1. Przy wytwarzaniu dokumentu niejawnego UE:

a) każdą stronę wyraźnie oznacza się klauzulą tajności;

b) numeruje się każdą stronę;

c) na dokumencie umieszcza się numer rejestracyjny i temat, który nie stanowi informacji niejawnej, chyba że z jego oznaczenia wynika inaczej;

d) na dokumencie umieszcza się datę;

e) na każdej stronie dokumentów z klauzulą tajności SECRET UE/EU SECRET lub wyższą, które mają zostać rozpowszechnione w kilku kopiach, umieszcza się numer kopii.

2. Jeżeli do EUCI nie można zastosować ustępu 1, podejmowane są inne odpowiednie środki zgodnie z przepisami wykonawczymi.

Artykuł 26

Obniżanie i znoszenie klauzul tajności EUCI

1. W momencie wytwarzania EUCI wytwórca wskazuje, o ile to możliwe, czy z daną datą lub w następstwie konkretnego wydarzenia klauzula tajności EUCI może zostać obniżona lub zniesiona.

2. Każdy departament Komisji przeprowadza regularne przeglądy EUCI, których jest wytwórcą, aby stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. Na podstawie przepisów wykonawczych ustanowiony zostaje system służący do przeglądu klauzul tajności nadanych zarejestrowanym EUCI wytworzonym w obrębie Komisji nie rzadziej niż co pięć lat. Przedmiotowy przegląd nie jest konieczny, jeżeli wytwórca wskazał na samym początku, że klauzula tajności nadana danym informacjom zostanie automatycznie obniżona lub zniesiona, a informacje te zostały odpowiednio oznaczone.

3. Po trzydziestu latach klauzula tajności RESTREINT UE/EU RESTRICTED, jaką oparzone są informacje wytworzone w Komisji, będzie uważana za automatycznie zniesiona zgodnie z rozporządzeniem (EWG, Euratom) nr 354/83 zmienionym rozporządzeniem Rady (WE, Euratom) nr 1700/2003 ([1]).

Artykuł 27

System kancelarii tajnych UE w Komisji

1. Bez uszczerbku dla art. 52 ust. 5 poniżej, w każdym departamencie Komisji, w którym korzysta się z EUCI opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET lub je przechowuje, określa się odpowiedzialną lokalną kancelarię tajną UE zapewniającą zgodność korzystania z EUCI z niniejszą decyzją.

2. Kancelaria tajna UE zarządzana przez Sekretariat Generalny stanowi główną kancelarię tajną UE Komisji. Kancelaria ta pełni funkcję:

— lokalnej kancelarii tajnej UE na porzeby Sekretariatu Generalnego Komisji;

— kancelarii tajnej UE na potrzeby prywatnych gabinetów członków Komisji, chyba że członkowie ci posiadają wyznaczoną lokalną kancelarię tajną UE;

— kancelarii tajnej UE na potrzeby dyrekcji generalnej lub służb nieposiadających żadnej lokalnej kancelarii tajnej UE;

— głównego punktu, do którego wpływają i z którego przekazywane są wszystkie informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED i wyższą, w tym SECRET UE/EU SECRET, wymieniane między Komisją, jej służbami i państwami trzecimi i organizacjami międzynarodowymi oraz, jeżeli jest to przewidziane w szczególnych ustaleniach, z innymi instytucjami, agencjami i organami UE.

3. Organ ds. bezpieczeństwa Komisji wyznacza w obrębie Komisji kancelarię tajną będącą głównym organem otrzymującym i przesyłającym informacje niejawne z klauzulą tajności TRES SECRET UE/EU TOP SECRET. W razie potrzeby można wyznaczyć podległe kancelarie tajne do wykorzystywania takich informacji do celów rejestracji.

4. Przedmiotowe podległe kancelarie tajne nie mogą przekazywać dokumentów z klauzulą tajności TRES SECRET UE/EU TOP SECRET bezpośrednio innym podległym kancelariom tajnym podlegającym tej samej głównej kancelarii tajnej TRES SECRET UE/EU TOP SECRET ani na zewnątrz bez wyraźnego pisemnego upoważnienia ze strony tej ostatniej.

5. Kancelarie tajne UE zostają ustanowione jako strefy bezpieczeństwa określone w rozdziale 3 i akredytuje je organ ds. akredytacji bezpieczeństwa Komisji (SAA).

Artykuł 28

Urzędnik kontroli kancelarii

1. Każda kancelaria tajna UE zarządzana jest przez urzędnika kontroli kancelarii.

2. Urzędnik kontroli kancelarii zostaje odpowiednio sprawdzony.

3. Urzędnik kontroli kancelarii podlega nadzorowi lokalnego pełnomocnika ochrony w ramach departamentu Komisji w zakresie stosowania przepisów dotyczących korzystania z dokumentów zawierających EUCI oraz przestrzegania odpowiednich przepisów bezpieczeństwa, standardów i wytycznych dotyczących bezpieczeństwa.

4. W zakresie swoich obowiązków dotyczących zarządzania kancelarią tajną UE, do której został przypisany, urzędnik kontroli kancelarii wykonuje, zgodnie z niniejszą decyzją i odpowiednimi przepisami, standardami i wytycznymi wykonawczymi, następujące ogólne zadania:

— zarządzanie czynnościami związanymi z rejestracją, konserwacją, powielaniem, tłumaczeniem, transmisją, wysyłaniem i niszczeniem lub przekazywaniem EUCI służbom archiwów historycznych;

— okresową weryfikację potrzeby utrzymania klauzuli tajności informacji;

— podejmuje się innych zadań związanych z ochroną EUCI określonych w ramach przepisów wykonawczych.

Artykuł 29

Rejestracja EUCI na potrzeby bezpieczeństwa

1. Do celów niniejszej decyzji rejestracja na potrzeby bezpieczeństwa (zwana dalej „rejestracją") oznacza stosowanie procedur rejestrowania etapów cyklu życia EUCI, w tym ich rozpowszechniania.

([1]) Rozporządzenie Rady (WE, Euratom) nr 1700/2003 z dnia 22 września 2003 r. zmieniające rozporządzenie (EWG, Euratom) nr 354/83 dotyczące udostępnienia do wglądu publicznego historycznych materiałów archiwalnych Europejskiej Wspólnoty Gospodarczej i Europejskiej Wspólnoty Energii Atomowej (Dz.U. L 243 z 27.9.2003, s. 1).

2. Wszystkie informacje lub materiały niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższą rejestruje się w wyznaczonych kancelariach tajnych w momencie ich wpłynięcia do jednostki organizacyjnej lub wysłania z tej jednostki.

3. W przypadku korzystania z EUCI lub ich przechowywania przy użyciu systemu teleinformatycznego (CIS) procedury rejestracji mogą być prowadzone w ramach procesów w obrębie samego CIS.

4. Bardziej szczegółowe przepisy dotyczące rejestracji EUCI na potrzeby bezpieczeństwa określono w przepisach wykonawczych.

Artykuł 30

Kopiowanie i tłumaczenie dokumentów niejawnych UE

1. Dokumenty z klauzulą tajności TRES SECRET UE/EU TOP SECRET nie mogą być kopiowane ani tłumaczone bez wcześniejszej pisemnej zgody ich wytwórcy.

2. Jeżeli wytwórca dokumentów niejawnych z klauzulą tajności SECRET UE/EU SECRET i niższą nie zgłosił oznaczeń zastrzegających w odniesieniu do ich kopiowania lub tłumaczenia, dokumenty takie można kopiować lub tłumaczyć na polecenie posiadacza.

3. Środki bezpieczeństwa, które mają zastosowanie do oryginalnego dokumentu, mają zastosowanie do jego kopii i tłumaczeń.

Artykuł 31

Przenoszenie EUCI

1. EUCI przenosi się w taki sposób, aby podczas przenoszenia chronić je przed nieuprawnionym ujawnieniem.

2. Przenoszenie EUCI podlega środkom ochronnym, które:

— są proporcjonalne do poziomu klauzuli tajności przenoszonych EUCI; oraz

— są dostosowane do szczególnych warunków ich przenoszenia, zależących w szczególności od faktu, czy EUCI są przenoszone:

  — w obrębie budynku Komisji lub grupy budynków Komisji stanowiącej zamkniętą całość;

  — między budynkami Komisji mieszczącymi się w tym samym państwie członkowskim;

  — na terytorium Unii;

  — z terytorium Unii na terytorium państwa trzeciego; oraz

  — są dostosowane do charakteru i formy EUCI.

3. Przedmiotowe środki ochronne określono szczegółowo w przepisach wykonawczych lub, w przypadku projektów i programów, o których mowa w art. 42, stanowią one integralną część odpowiednich instrukcji bezpieczeństwa programu lub projektu.

4. Przepisy wykonawcze lub instrukcje bezpieczeństwa programu lub projektu zawierają przepisy proporcjonalne do poziomu klauzuli tajności EUCI w odniesieniu do:

— sposobu ich przenoszenia, np. osobiście, za pośrednictwem kurierów dyplomatycznych lub wojskowych, za pośrednictwem usług pocztowych lub prywatnych służb kurierskich;

— pakowania EUCI;

— technicznych środków przeciwdziałania w przypadku przenoszenia EUCI na nośnikach elektronicznych;

— wszystkich innych środków proceduralnych, fizycznych lub elektronicznych;

— procedur rejestracji;

— wykorzystania pracowników posiadających upoważnienie w zakresie bezpieczeństwa.

5. W przypadku przenoszenia EUCI na nośnikach elektronicznych, niezależnie od przepisów art. 21 ust. 5, środki ochronne określone w odpowiednich przepisach wykonawczych mogą być uzupełnione o odpowiednie techniczne środki przeciwdziałania zatwierdzone przez organ ds. bezpieczeństwa Komisji, co pozwoli zminimalizować ryzyko utraty lub narażenia na szwank bezpieczeństwa informacji.

Artykuł 32

Niszczenie EUCI

1. Dokumenty niejawne UE, które nie są już potrzebne, mogą zostać zniszczone z uwzględnieniem przepisów dotyczących archiwizowania oraz zasad i przepisów Komisji dotyczących zarządzania dokumentami i archiwizowania, a w szczególności zgodnie ze wspólnym wykazem zatrzymywanych danych na poziomie Komisji.

2. EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą są niszczone przez urzędnika kontroli kancelarii odpowiedniej kancelarii tajnej UE na polecenie posiadacza lub właściwego organu. Urzędnik kontroli kancelarii odpowiednio aktualizuje rejestry i inne informacje dotyczące rejestracji.

3. W odniesieniu do dokumentów niejawnych z klauzulą tajności SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET niszczenia dokonuje urzędnik kontroli kancelarii w obecności świadka posiadającego poświadczenie bezpieczeństwa co najmniej na poziomie klauzuli tajności niszczonego dokumentu.

4. Osoba dokonująca rejestracji oraz świadek, jeżeli jego obecność jest wymagana, podpisują protokół zniszczenia, który zostaje włączony do dokumentacji kancelarii tajnej. Urzędnik kontroli odpowiedniej kancelarii tajnej UE przechowuje protokoły zniszczenia dokumentów z klauzulą tajności TRES SECRET UE/EU TOP SECRET przez okres co najmniej dziesięciu lat, a dokumentów niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET przez okres co najmniej pięciu lat.

5. Dokumenty niejawne, w tym dokumenty z klauzulą tajności RESTREINT UE/EU RESTRICTED, są niszczone z zastosowaniem metod, które określono w przepisach wykonawczych i które spełniają odpowiednie standardy UE lub równoważne.

6. Niszczenie komputerowych nośników EUCI odbywa się zgodnie z procedurami określonymi w przepisach wykonawczych.

Artykuł 33

Niszczenie EUCI w sytuacjach nadzwyczajnych

1. Departamenty Komisji posiadające EUCI są zobowiązane do opracowania dostosowanych do lokalnych uwarunkowań planów ochrony materiałów niejawnych UE w sytuacjach kryzysowych, uwzględniających możliwość podjęcia w razie potrzeby działań takich jak zniszczenie w trybie nagłym lub plany ewakuacji. Rozpowszechniają one instrukcje postępowania, które uznają za konieczne, aby zapobiec dostaniu się EUCI w niepowołane ręce.

2. Ustalenia dotyczące ochrony lub niszczenia materiałów z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET w sytuacji kryzysowej w żadnym wypadku nie wpływają niekorzystnie na ochronę lub niszczenie materiałów z klauzulą tajności TRES SECRET UE/EU TOP SECRET, w tym urządzeń szyfrujących; ich ochrona ma pierwszeństwo w stosunku do wszelkich innych działań.

3. W sytuacji nadzwyczajnej, jeżeli istnieje bezpośrednie ryzyko nieuprawnionego ujawnienia, EUCI są niszczone przez posiadacza w taki sposób, aby nie mogły zostać odtworzone w całości ani częściowo. Wytwórca i kancelaria tajna wytwórcy zostają powiadomieni o zniszczeniu zarejestrowanych EUCI w trybie nagłym.

4. Bardziej szczegółowe postanowienia dotyczące niszczenia EUCI określono w przepisach wykonawczych.

ROZDZIAŁ 5

OCHRONA INFORMACJI NIEJAWNYCH UE W SYSTEMACH TELEINFORMATYCZNYCH (CIS)

Artykuł 34

Podstawowe zasady zabezpieczania informacji

1. Zabezpieczanie informacji w kontekście systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, które są w nich przetwarzane, i będą działać tak jak powinny i kiedy powinny pod kontrolą uprawnionych użytkowników.

2. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom:

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

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

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

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

niezaprzeczalności: możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia.

3. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.

Artykuł 35

Definicje

Do celów niniejszego rozdziału stosuje się poniższe definicje:

a) „akredytacja" oznacza formalne upoważnienie i zezwolenie przyznane systemowi teleinformatycznemu przez organ ds. akredytacji bezpieczeństwa (SAA) na przetwarzanie EUCI w środowisku operacyjnym tego systemu w następstwie formalnego zatwierdzenia planu bezpieczeństwa i jego prawidłowego wdrożenia;

b) „procedura akredytacji" oznacza konieczne etapy i zadania wymagane przed przyznaniem akredytacji przez organ ds. akredytacji bezpieczeństwa. Te etapy i zadania są określone w standardzie procedury akredytacji;

c) „system teleinformatyczny" (CIS) oznacza system umożliwiający korzystanie z informacji w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, pracowników oraz zasoby informatyczne;

d) „ryzyko szczątkowe" oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa, z uwagi na to, że nie przeciwdziała się wszystkim zagrożeniom i że nie każdą podatność można wyeliminować;

e) „ryzyko" oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu przez nią używanego i przez to wyrządzi szkodę tej organizacji i jej zasobom materialnym lub niematerialnym. Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków;

f) „akceptacja ryzyka" jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

g) „ocena ryzyka" polega na określaniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

h) „informowanie o ryzyku" polega na upowszechnianiu wiedzy o ryzyku wśród społeczności korzystających z CIS, na informowaniu o takim ryzyku organów zatwierdzających i na składaniu sprawozdań z takiego ryzyka organom operacyjnym;

i) „zmniejszanie ryzyka" polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych), jego przenoszeniu lub monitorowaniu.

Artykuł 36

CIS, w których korzysta się z EUCI

1. CIS przetwarza EUCI zgodnie z koncepcją zabezpieczania informacji.

2. W przypadku CIS, w których korzysta się z EUCI, zgodność z polityką Komisji w dziedzinie bezpieczeństwa systemów informatycznych, o której mowa w decyzji C(2006) 3602 ([1]), oznacza, że:

a) w odniesieniu do realizacji polityki w zakresie bezpieczeństwa systemów informatycznych w całym cyklu życia systemu informacyjnego stosuje się podejście Planuj – Wykonaj – Sprawdź – Działaj;

b) potrzeby w zakresie bezpieczeństwa muszą zostać określone z zastosowaniem oceny wpływu na działalność;

c) system informacyjny i zawarte w nim dane muszą być poddane formalnej klasyfikacji aktywów;

([1]) Decyzja C(2006) 3602 z dnia 16 sierpnia 2006 r. dotycząca bezpieczeństwa systemów informacyjnych wykorzystywanych przez Komisję Europejską.

d) wszystkie obowiązkowe środki bezpieczeństwa określone w ramach polityki w dziedzinie bezpieczeństwa systemów informatycznych muszą zostać wdrożone;

e) musi zostać zastosowany proces zarządzania ryzykiem, który składa się z następujących etapów: identyfikacja zagrożeń i podatności, ocena ryzyka, zmniejszenie ryzyka, akceptacja ryzyka i informowanie o ryzyku;

f) określa się, wdraża, sprawdza i poprawia plan bezpieczeństwa, w tym politykę bezpieczeństwa i procedurę bezpiecznej eksploatacji systemu.

3. Wszyscy pracownicy zaangażowani w projektowanie, budowę, testowanie, funkcjonowanie, zarządzanie lub stosowanie CIS, w których przetwarzane są EUCI, zgłaszają SAA wszelkie ewentualne niedoskonałości w zakresie bezpieczeństwa, incydenty, naruszenia lub narażenia na szwank bezpieczeństwa, które mogą mieć wpływ na ochronę CIS lub znajdujących się w nich EUCI.

4. Jeżeli EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane w następujący sposób:

a) pierwszeństwo przyznaje się produktom zatwierdzonym przez Radę lub Sekretarza Generalnego Rady Unii Europejskiej, działającego jako organ ds. zatwierdzania produktów kryptograficznych Rady, na podstawie zalecenia Grupy Ekspertów ds. Bezpieczeństwa Komisji;

b) jeżeli uzasadniają to określone względy operacyjne, organ Komisji ds. zatwierdzania produktów kryptograficznych (CAA) może, na podstawie zalecenia Grupy Ekspertów ds. Bezpieczeństwa Komisji, znieść wymogi wynikające z lit. a) i udzielić tymczasowej akceptacji na dany okres.

5. Podczas transmisji EUCI drogą elektroniczną, ich przetwarzania i przechowywania na nośnikach elektronicznych stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w okolicznościach nadzwyczajnych zastosowanie mogą mieć szczególne procedury lub szczególne konfiguracje techniczne zatwierdzone przez CAA.

6. Wdrażane są specjalne środki bezpieczeństwa w celu ochrony CIS przetwarzającego informacje niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą przed narażeniem tych informacji na szwank z powodu niezamierzonych emisji elektromagnetycznych (tzw. „środki bezpieczeństwa TEMPEST"). Takie środki bezpieczeństwa są proporcjonalne do ryzyka wykorzystania informacji niejawnych i do poziomu klauzuli tajności.

7. Organ ds. bezpieczeństwa Komisji obejmuje następujące funkcje:

— organu ds. zabezpieczania informacji (IAA);

— organu ds. akredytacji bezpieczeństwa (SAA);

— organu ds. TEMPEST (TA);

— organu ds. zatwierdzania produktów kryptograficznych (CAA);

— organu ds. dystrybucji produktów kryptograficznych (CDA).

8. Organ ds. bezpieczeństwa Komisji wyznacza dla każdego systemu operacyjny organ ds. zabezpieczania informacji.

9. Obowiązki w ramach funkcji opisanych w ust. 7 i 8 określone zostaną w przepisach wykonawczych.

Artykuł 37

Akredytacja CIS, w których korzysta się z EUCI

1. Wszystkie CIS, w których korzysta się z EUCI, poddawane są procedurze akredytacji na podstawie zasad zabezpieczania informacji; poziom ich szczegółowości musi być proporcjonalny do poziomu wymaganej ochrony.

2. Procedura akredytacji obejmuje formalne zatwierdzenie przez organ ds. akredytacji bezpieczeństwa Komisji planu bezpieczeństwa dla danego CIS w celu uzyskania pewności, że:

a) proces zarządzania ryzykiem, o którym mowa w art. 36 ust. 2, został odpowiednio przeprowadzony;

b) właściciel systemu świadomie zaakceptował ryzyko szczątkowe; oraz

c) osiągnięto wystarczający poziom ochrony CIS i przetwarzanych w nim EUCI zgodnie z niniejszą decyzją.

3. Organ Komisji ds. akredytacji bezpieczeństwa wydaje świadectwo akredytacji określające najwyższą klauzulę tajności EUCI, które mogą być przetwarzane w danym CIS, a także odpowiednie warunki jego działania. Nie narusza to zadań powierzonych Radzie Akredytacji w zakresie Bezpieczeństwa i określonych w art. 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 512/2014 ([1]).

4. Wspólna Rada Akredytacji w zakresie Bezpieczeństwa jest odpowiedzialna za udzielanie akredytacji CIS Komisji, w funkcjonowanie którego zaangażowanych jest kilka stron. W skład tej rady wchodzi po jednym przedstawicielu SAA z każdej zaangażowanej strony, a jej obradom przewodniczy przedstawiciel SAA ze strony Komisji.

5. Procedura akredytacji obejmuje szereg zadań, które muszą wykonać zaangażowane strony. Odpowiedzialność za przygotowywanie dokumentacji akredytacyjnej spoczywa całkowicie na właścicielu systemu CIS.

6. Za akredytację odpowiedzialny jest organ Komisji ds. akredytacji bezpieczeństwa, który na każdym etapie cyklu życia CIS ma prawo do:

a) zażądania zastosowania procesu akredytacji;

b) przeprowadzenia audytu lub inspekcji CIS;

c) w przypadku gdy przestały być spełnione warunki działania – zażądania określenia planu poprawy bezpieczeństwa i jego skutecznego wdrożenia w ściśle określonych ramach czasowych, ewentualnego wycofania zezwolenia na eksploatację CIS do momentu, w którym warunki działania zostaną ponownie spełnione.

7. Procedurę akredytacji określono w standardzie procedury akredytacji dla CIS, w którym przetwarzane są EUCI; zostaje on przyjęty zgodnie z art.10 ust. 3 decyzji C(2006) 3602.

Artykuł 38

Okoliczności nadzwyczajne

1. Niezależnie od przepisów niniejszego rozdziału w okolicznościach nadzwyczajnych, takich jak zbliżający się lub trwający kryzys, konflikt, stan wojny, lub w wyjątkowych sytuacjach operacyjnych można stosować specjalne procedury opisane poniżej.

2. EUCI można transmitować z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli tajności lub w postaci niezaszyfrowanej za zgodą właściwego organu, jeżeli jakakolwiek zwłoka spowodowałaby szkody wyraźnie większe od szkód, które mogłoby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:

a) nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego; oraz

b) materiały niejawne nie mogą być dostarczone na czas w inny sposób.

3. Informacje niejawne transmitowane w okolicznościach przedstawionych w ust. 1 nie są opatrzone żadnymi oznaczeniami ani wskazaniami odróżniającymi je od informacji jawnych lub informacji, które mogą być chronione przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy są bezzwłocznie powiadamiani za pomocą innych środków o poziomie klauzuli tajności.

4. Następnie sporządzane jest sprawozdanie dla właściwego organu i Grupy Ekspertów ds. Bezpieczeństwa Komisji.

ROZDZIAŁ 6

BEZPIECZEŃSTWO PRZEMYSŁOWE

Artykuł 39

Podstawowe zasady

1. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę EUCI

a) w ramach umów niejawnych przez:

   (i) kandydatów lub oferentów w procedurze przetargowej i w postępowaniu o udzielenie zamówienia;

   (ii) wykonawców i podwykonawców na wszystkich etapach cyklu życia umów niejawnych;

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 512/2014 z dnia 16 kwietnia 2014 r. zmieniające rozporządzenie (UE) nr 912/2010 ustanawiające Agencję Europejskiego GNSS (Dz.U. L 150 z 20.5.2014, s. 72).

b) w ramach niejawnych umów o udzielenie dotacji przez:

(i) wnioskodawców przez cały okres trwania procedury przyznawania dotacji;

(ii) beneficjentów na wszystkich etapach cyklu życia niejawnych umów o udzielenie dotacji.

2. Przedmiotowe umowy lub umowy o udzielenie dotacji nie obejmują dostępu do informacji z klauzulą tajności TRES SECRET UE/EU TOP SECRET.

3. O ile nie określono inaczej, przepisy zawarte w niniejszym rozdziale dotyczące umów lub wykonawców niejawnych mają zastosowanie również do niejawnych umów o podwykonawstwo lub do podwykonawców.

Artykuł 40

Definicje

Na użytek niniejszego rozdziału stosuje się następujące definicje:

a) „umowa niejawna" oznacza umowę ramową lub umowę, o której mowa w rozporządzeniu Rady (WE, Euratom) nr 1605/2002 ([1]), zawieraną przez Komisję lub jeden z jej departamentów z wykonawcą na dostawę ruchomości lub nieruchomości, wykonanie robót lub świadczenie usług, której wykonanie wymaga wytwarzania, wykorzystywania lub przechowywania EUCI lub wiąże się z ich wytwarzaniem, wykorzystywaniem i przechowywaniem;

b) „niejawna umowa o podwykonawstwo" oznacza umowę ramową lub umowę zawieraną przez wykonawcę Komisji lub jednego z jej departamentów z innym wykonawcą (np. podwykonawcą) na dostawę ruchomości lub nieruchomości, wykonanie robót lub świadczenie usług, której wykonanie wymaga wytwarzania, wykorzystywania lub przechowywania EUCI lub wiąże się z ich wytwarzaniem, wykorzystywaniem i przechowywaniem;

c) „niejawna umowa o udzielenie dotacji" oznacza umowę, na podstawie której Komisja przyznaje dotację, jak określono w części I, tytule VI rozporządzenia (WE, Euratom) nr 1605/2002, której wykonanie wymaga wytwarzania, wykorzystywania lub przechowywania EUCI lub wiąże się z ich wytwarzaniem, wykorzystywaniem i przechowywaniem;

d) „wyznaczona władza bezpieczeństwa" (WWB) oznacza instytucję podlegającą krajowej władzy bezpieczeństwa (KWB) w państwie członkowskim, odpowiedzialną za przekazywanie podmiotom gospodarczym lub innym informacji dotyczących krajowej polityki we wszelkich sprawach związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w jej realizacji. Zadania WWB może wykonywać KWB lub dowolny inny właściwy organ.

Artykuł 41

Procedura dotycząca umów niejawnych i niejawnych umów o udzielenie dotacji

1. Każdy departament Komisji zapewnia, jako instytucja zamawiająca, by w przypadku zawierania umów niejawnych lub niejawnych umów o udzielenie dotacji wprowadzano do nich minimalne standardy bezpieczeństwa przemysłowego lub odniesienie do tych standardów, a także by przestrzegano ich przy udzielaniu zamówienia niejawnego lub zawieraniu niejawnej umowy o udzielenie dotacji.

2. Do celów ust. 1 właściwe służby w obrębie Komisji korzystają z doradztwa Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, a w szczególności Dyrekcji ds. Bezpieczeństwa, oraz zapewniają, by modele umów i umów o podwykonawstwo oraz modele umów o udzielenie dotacji obejmowały przepisy odzwierciedlające podstawowe zasady i minimalne standardy dotyczące ochrony EUCI, które powinni spełniać wykonawcy i podwykonawcy oraz odpowiednio beneficjenci umów o udzielenie dotacji.

3. Komisja ściśle współpracuje z KWB, WWB lub każdym innym właściwym organem danego państwa członkowskiego.

4. Jeżeli instytucja zamawiająca zamierza uruchomić procedurę mającą na celu zawarcie umowy niejawnej lub niejawnej umowy o udzielenie dotacji, korzysta z doradztwa organu ds. bezpieczeństwa Komisji w zakresie kwestii odnoszących się do niejawnego charakteru procedury i jej elementów na wszystkich jej etapach.

5. Wzory i modele niejawnych umów i umów o podwykonawstwo, niejawnych umów o udzielenie dotacji, ogłoszeń o zamówieniach, wskazówki dotyczące przypadków, w których wymagane są świadectwa bezpieczeństwa przemysłowego (SBP), instrukcje bezpieczeństwa programu lub projektu (IBP), dokumenty określające aspekty bezpieczeństwa (DOAB), wizyty, transmisja i przemieszczanie EUCI w ramach umów niejawnych lub niejawnych umów o udzielenie dotacji są określone w przepisach wykonawczych dotyczących bezpieczeństwa przemysłowego po uprzedniej konsultacji z Grupą Ekspertów ds. Bezpieczeństwa Komisji.

([1]) Rozporządzenie Rady (WE, Euratom) nr 1605/2002 z dnia 25 czerwca 2002 r. w sprawie rozporządzenia finansowego mającego zastosowanie do budżetu ogólnego Wspólnot Europejskich (Dz.U. L 248 z 16.9.2002, s. 1).

6. Komisja może zawierać umowy niejawne lub niejawne umowy o udzielenie dotacji, na podstawie których powierza się zadania obejmujące EUCI lub wiążące się z dostępem do tych informacji, korzystaniem z nich lub ich przechowywaniem przez podmioty gospodarcze zarejestrowane w państwie członkowskim lub w państwie trzecim, z którym, zgodnie z rozdziałem 7. niniejszej decyzji, zawarto umowę lub porozumienie administracyjne.

Artykuł 42

Elementy dotyczące bezpieczeństwa w umowie niejawnej lub niejawnej umowie o udzielenie dotacji

1. Umowy niejawne i niejawne umowy o udzielenie dotacji obejmują następujące elementy dotyczące bezpieczeństwa:

Instrukcje bezpieczeństwa programu lub projektu

a) „Instrukcje bezpieczeństwa programu lub projektu (IBP)" oznaczają wykaz procedur bezpieczeństwa stosowanych w odniesieniu do określonego programu lub projektu w celu normalizacji procedur bezpieczeństwa. Instrukcje mogą być zmieniane podczas trwania programu lub projektu.

b) Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa opracowuje ogólne IBP; departamenty Komisji odpowiedzialne za programy lub projekty obejmujące postępowanie z EUCI lub ich przechowywanie mogą opracowywać, w stosownych przypadkach, szczegółowe IBP oparte na ogólnych IBP.

c) Szczegółowe IBP są opracowywane zwłaszcza w odniesieniu do programów i projektów charakteryzujących się znacznym zakresem, skalą i złożonością, lub mnogością bądź zróżnicowaniem wykonawców, beneficjentów i innych zaangażowanych partnerów i zainteresowanych stron, np. w odniesieniu do ich statusu prawnego. Departament(-y) Komisji zarządzający(-ące) programem lub projektem w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa opracowują szczegółowe IBP.

d) W celu uzyskania porady Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przedstawia ogólne i szczegółowe IBP Grupie Ekspertów ds. Bezpieczeństwa Komisji.

Dokument określający aspekty bezpieczeństwa

a) „Dokument określający aspekty bezpieczeństwa" (DOAB) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część każdej umowy niejawnej obejmującej dostęp do EUCI lub ich wytwarzanie, określający wymogi bezpieczeństwa i wskazujący te elementy umowy, których bezpieczeństwo wymaga ochrony.

b) W DOAB opisane są wymogi bezpieczeństwa dotyczące poszczególnych umów. W stosownych przypadkach DOAB zawiera przewodnik nadawania klauzul (PNK) i stanowi integralną część umowy niejawnej lub niejawnej umowy o podwykonawstwo bądź niejawnej umowy o udzielenie dotacji.

c) DOAB zawiera przepisy zobowiązujące wykonawcę lub beneficjenta do przestrzegania minimalnych standardów określonych w niniejszej decyzji. Instytucja zamawiająca zapewnia, by w DOAB zostało wskazane, że nieprzestrzeganie tych minimalnych standardów może stanowić wystarczający powód do rozwiązania umowy lub umowy o udzielenie dotacji.

2. Zarówno IBP, jak i DOAB obejmują obowiązkowy element dotyczący bezpieczeństwa w postaci PNK:

a) „Przewodnik nadawania klauzul" (PNK) oznacza dokument opisujący niejawne elementy programu, projektu, umowy lub umowy o udzielenie dotacji, określający poziomy klauzuli tajności, które mają zastosowanie. PNK może być rozszerzany przez cały czas trwania programu, projektu, umowy lub umowy o udzielenie dotacji, a klauzule tajności dla elementów informacji mogą podlegać zmianie lub obniżeniu; jeżeli PNK istnieje, to stanowi część DOAB.

b) Przed ogłoszeniem zaproszenia do składania ofert lub zawarciem umowy niejawnej departament Komisji jako instytucja zamawiająca określa klauzulę tajności wszelkich informacji, których należy udzielić kandydatom i oferentom lub wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym celu, po konsultacji z organem ds. bezpieczeństwa Komisji, departament opracowuje PNK, który należy stosować podczas realizacji umowy zgodnie z niniejszą decyzją i jej przepisami wykonawczymi.

c) Do określania klauzuli tajności różnych elementów umowy niejawnej zastosowanie mają następujące zasady:

(i) podczas opracowywania PNK departament Komisji jako instytucja zamawiająca uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę tajności nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie do celów umowy zatwierdził;

(ii) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności któregokolwiek z jej elementów; oraz

(iii) w stosownych przypadkach instytucja zamawiająca kontaktuje się za pośrednictwem organu ds. bezpieczeństwa Komisji z KWB, WWB państw członkowskich lub jakimkolwiek innym właściwym organem bezpieczeństwa w razie jakichkolwiek zmian klauzul tajności informacji wytworzonych przez wykonawców lub przekazanych im podczas realizacji umowy oraz w przypadku wprowadzania jakichkolwiek późniejszych zmian do PNK.

Artykuł 43

Dostęp pracowników zatrudnionych przez wykonawców i przez beneficjentów do EUCI

Instytucja zamawiająca lub udzielająca dotacji zapewnia, aby umowa niejawna lub niejawna umowa o udzielenie dotacji obejmowała przepisy wskazujące, że personel wykonawcy, podwykonawcy lub beneficjenta, który do realizacji umowy niejawnej, niejawnej umowy o podwykonawstwo lub niejawnej umowy o udzielenie dotacji potrzebuje dostępu do EUCI, uzyskuje taki dostęp, pod warunkiem że:

a) posiada upoważnienie w zakresie bezpieczeństwa do odpowiedniego poziomu lub został odpowiednio upoważniony w inny sposób w wyniku ustalenia jego potrzeb w ramach zasady ograniczonego dostępu;

b) został poinformowany o obowiązujących przepisach bezpieczeństwa służących ochronie EUCI i potwierdził, że zapoznał się ze swoimi obowiązkami w zakresie ochrony takich informacji;

c) otrzymał od KWB, WWB lub jakiegokolwiek innego właściwego organu poświadczenie bezpieczeństwa do odpowiedniego poziomu informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.

Artykuł 44

Świadectwo bezpieczeństwa przemysłowego

1. „Świadectwo bezpieczeństwa przemysłowego" (SBP) oznacza wydane w trybie administracyjnym oświadczenie KWB, WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiedni poziom ochrony EUCI do określonego poziomu klauzuli tajności.

2. SBP wydawane przez KWB lub WWB, lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego w celu zaświadczenia zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot gospodarczy jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET), są przedstawiane organowi ds. bezpieczeństwa Komisji, który przekazuje je departamentowi Komisji pełniącemu rolę instytucji zamawiającej lub udzielającej dotacji, zanim kandydat, oferent lub wnioskodawca lub podmiot występujący o dotację lub beneficjent uzyska dostęp do EUCI.

3. W stosownych przypadkach instytucja zamawiająca powiadamia za pośrednictwem organu ds. bezpieczeństwa Komisji odpowiednią KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa, że do realizacji umowy wymagane jest SBP. SBP lub PBO są wymagane, jeżeli podczas postępowania o udzielenie zamówień lub podczas procedury przyznawania dotacji mają być dostarczone EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.

4. Instytucja zamawiająca lub udzielająca dotacji nie zawiera umowy niejawnej lub niejawnej umowy o udzielenie dotacji z wybranym oferentem lub uczestnikiem, zanim nie otrzyma od KWB, WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca, potwierdzenia, że wydane zostało odpowiednie SBP, jeżeli istnieje taki wymóg.

5. W przypadku gdy KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa, który wydał SBP, powiadomił organ ds. bezpieczeństwa Komisji o zmianach wpływających na SBP, organ ten informuje departament Komisji pełniący funkcję instytucji zamawiającej lub udzielającej dotacji. W przypadku umowy o podwykonawstwo odpowiednio informowane są KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa.

6. Cofnięcie SBP przez właściwą KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa stanowi dla instytucji zamawiającej lub udzielającej dotacji wystarczający powód do rozwiązania umowy niejawnej lub wykluczenia kandydata, oferenta lub wnioskodawcy z postępowania. W tym celu w modelach umów i modelach umów o udzielenie dotacji, które mają być opracowane, uwzględnia się stosowny przepis.

Artykuł 45

Przepisy dotyczące umów niejawnych i niejawnych umów o udzielenie dotacji

1. Jeżeli EUCI są przekazywane kandydatowi, oferentowi lub wnioskodawcy podczas postępowania o udzielenie zamówień, zaproszenie do składania ofert lub zaproszenie do składania wniosków zawiera przepis zobowiązujący kandydata, oferenta lub wnioskodawcę, który nie złoży oferty lub wniosku lub który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.

2. Instytucja zamawiająca lub udzielająca dotacji powiadamia – za pośrednictwem organu ds. bezpieczeństwa Komisji – właściwe KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o zawarciu umowy niejawnej lub niejawnej umowy o udzielenie dotacji oraz o istotnych danych, takich jak nazwisko wykonawcy(-ów) lub beneficjentów, okres obowiązywania umowy oraz maksymalny poziom klauzuli tajności.

3. W przypadku rozwiązania takich umów lub umów o udzielenie dotacji instytucja zamawiająca lub udzielająca dotacji niezwłocznie powiadamia o tym fakcie – za pośrednictwem organu ds. bezpieczeństwa Komisji – KWB, WWB lub jakikolwiek inny właściwy organ ds. bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub beneficjent dotacji.

4. Z reguły po rozwiązaniu umowy niejawnej lub niejawnej umowy o udzielenie dotacji lub po wypowiedzeniu uczestnictwa przez beneficjenta dotacji wymaga się od wykonawcy lub beneficjenta dotacji zwrócenia wszelkich posiadanych przezeń EUCI na ręce instytucji zamawiającej lub udzielającej dotacji.

5. W DOAB określa się szczególne przepisy dotyczące usuwania EUCI podczas wykonywania umowy niejawnej lub niejawnej umowy o udzielenie dotacji lub po jej rozwiązaniu.

6. Jeżeli wykonawca lub beneficjent dotacji są upoważnieni do zachowania EUCI po rozwiązaniu umowy niejawnej lub niejawnej umowy o udzielenie dotacji, wykonawca lub beneficjent dotacji nadal przestrzegają minimalnych standardów zawartych w niniejszej decyzji oraz nadal chronią poufność EUCI.

Artykuł 46

Szczególne przepisy dotyczące umów niejawnych

1. Istotne dla ochrony EUCI warunki, na których wykonawca może zlecić podwykonawstwo, są określone w zaproszeniu do składania ofert oraz w umowie niejawnej.

2. Przed zleceniem podwykonawstwa którychkolwiek części umowy niejawnej wykonawca uzyskuje zgodę instytucji zamawiającej. Umowa o podwykonawstwo wiążąca się z dostępem do EUCI nie może być zawarta z podwykonawcą zarejestrowanym w państwie trzecim, chyba że istnieją ramy prawne dotyczące bezpieczeństwa informacji, jak przewidziano w rozdziale 7.

3. Wykonawca odpowiada za zapewnienie zgodności wszystkich podejmowanych w ramach podwykonawstwa czynności z minimalnymi standardami określonymi w niniejszej decyzji i nie dostarcza podwykonawcy EUCI bez uprzedniej pisemnej zgody instytucji zamawiającej.

4. Jeżeli chodzi o EUCI wytworzone lub wykorzystywane przez wykonawcę, za ich wytwórcę uznaje się Komisję, a prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

Artykuł 47

Wizyty związane z umowami niejawnymi

1. Jeżeli w związku z wykonaniem umowy niejawnej lub niejawnej umowy o udzielenie dotacji pracownik Komisji bądź personel wykonawcy lub personel beneficjenta dotacji musi uzyskać dostęp do informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w obiektach drugiej strony, organizowane są wizyty we współpracy z KWB, WWB lub z jakimkolwiek innym właściwym organem bezpieczeństwa. O takich wizytach informuje się organ ds. bezpieczeństwa Komisji. KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa może uzgodnić procedurę umożliwiającą bezpośrednie organizowanie wizyt w kontekście konkretnych programów lub projektów.

2. Wszystkie osoby wizytujące posiadają odpowiednie poświadczenie bezpieczeństwa i kierują się zasadą ograniczonego dostępu do EUCI związanych z umową niejawną.

3. Osobom wizytującym umożliwia się dostęp wyłącznie do EUCI związanych z celem wizyty.

4. Bardziej szczegółowe przepisy określono w przepisach wykonawczych.

5. Zgodność z przepisami dotyczącymi wizyt związanych z umowami niejawnymi, określonymi w niniejszej decyzji i w jej przepisach wykonawczych, o których mowa w ust. 4, jest obowiązkowa.

Artykuł 48

Transmisja i przemieszczanie EUCI w związku z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji

1. Do transmisji EUCI drogą elektroniczną zastosowanie mają odpowiednie przepisy rozdziału 5. niniejszej decyzji.

2. Do przemieszczania EUCI zastosowanie mają odpowiednie przepisy rozdziału 4. niniejszej decyzji i jej przepisy wykonawcze zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

3. Jeżeli materiały niejawne są transportowane jako ładunek, do określania zabezpieczeń stosuje się następujące zasady:

a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do miejsca przeznaczenia;

b) stopień ochrony, jakim objęto przesyłkę, określa się według najwyższego poziomu klauzuli tajności materiału zawartego w przesyłce;

c) przed jakimkolwiek transgranicznym przemieszczeniem materiałów niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, nadawca sporządza plan przewozu, który jest zatwierdzany przez KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa;

d) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i kończą się tak szybko, jak pozwolą na to okoliczności;

e) jeżeli jest to możliwe, trasy powinny przebiegać wyłącznie przez terytoria państw członkowskich. Transport trasami przebiegającymi przez terytoria państw innych niż państwa członkowskie powinien się odbywać wyłącznie pod warunkiem zatwierdzenia przez KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa zarówno państwa nadawcy, jak i państwa odbiorcy.

Artykuł 49

Przekazywanie EUCI wykonawcom i beneficjentom dotacji znajdującym się w państwach trzecich

EUCI są przekazywane wykonawcom lub beneficjentom dotacji znajdującym się w państwach trzecich zgodnie ze środkami bezpieczeństwa uzgodnionymi między organem ds. bezpieczeństwa Komisji, departamentem Komisji jako instytucją zamawiającą lub przyznającą dotację oraz KWB, WWB lub jakimkolwiek innym właściwym organem bezpieczeństwa danego państwa trzeciego, w którym zarejestrowany jest wykonawca lub beneficjent dotacji.

Artykuł 50

Postępowanie z informacjami niejawnymi z klauzulą tajności UE/EU RESTRICTED w kontekście umów niejawnych lub niejawnych umów o udzielenie dotacji

1. Ochrona informacji niejawnych z klauzulą tajności UE/EU RESTRICTED wykorzystywanych lub przechowywanych w ramach umów niejawnych lub umów o udzielenie dotacji opiera się na zasadzie proporcjonalności i uzyskiwania najlepszych efektów z danych nakładów.

2. W kontekście umów niejawnych lub niejawnych umów o udzielenie dotacji związanych z wykorzystywaniem informacji niejawnych opatrzonych klauzulą tajności UE/EU RESTRICTED nie wymaga się SBP lub PBO.

3. Jeżeli umowa lub umowa o udzielenie dotacji wiąże się z przetwarzaniem informacji niejawnych z klauzulą tajności RESTREINT UE/EU RESTRICTED w CIS, który eksploatuje wykonawca lub beneficjent dotacji, instytucja zamawiająca lub przyznająca dotację zapewnia, po konsultacji z organem ds. bezpieczeństwa Komisji, aby umowa lub umowa o udzielenie dotacji określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji lub zatwierdzenia CIS proporcjonalnie do szacowanego ryzyka, uwzględniając wszystkie odpowiednie czynniki. Zakres akredytacji lub zatwierdzenia w przypadku takiego CIS jest uzgadniany między organem ds. bezpieczeństwa Komisji a odpowiednią KWB lub WWB.

ROZDZIAŁ 7

WYMIANA INFORMACJI NIEJAWNYCH Z INNYMI INSTYTUCJAMI, AGENCJAMI, ORGANAMI I BIURAMI UE, Z PAŃSTWAMI CZŁONKOWSKIMI ORAZ PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

Artykuł 51

Podstawowe zasady

1. Jeżeli Komisja lub jeden z jej departamentów stwierdza, że zachodzi konieczność wymiany EUCI z inną instytucją, agencją, organem lub biurem UE bądź z państwem trzecim lub organizacją międzynarodową, podejmuje się niezbędne kroki w celu ustanowienia odpowiednich ram prawnych lub administracyjnych takiej wymiany, do których należeć mogą umowy o bezpieczeństwie informacji lub porozumienia administracyjne zawarte zgodnie z odpowiednimi przepisami.

2. Nie naruszając postanowień art. 57, EUCI wymienia się z inną instytucją, agencją, organem lub biurem UE lub z państwem trzecim lub organizacją międzynarodową tylko pod warunkiem, że istnieją przedmiotowe odpowiednie ramy prawne lub administracyjne, a także dostateczne gwarancje, że dana instytucja, agencja, organ lub biuro UE bądź państwo trzecie lub organizacja międzynarodowa stosuje równoważne podstawowe zasady i minimalne standardy ochrony informacji niejawnych.

Artykuł 52

Wymiana EUCI z innymi instytucjami, agencjami, organami i biurami UE

1. Przed zawarciem porozumienia administracyjnego dotyczącego wymiany EUCI z inną instytucją, agencją, organem lub biurem UE Komisja upewnia się, czy dana instytucja, agencja, organ lub biuro UE:

a) posiada ramy prawne służące ochronie EUCI, które określają podstawowe zasady i minimalne standardy równoważne zasadom i standardom określonym w niniejszej decyzji i jej przepisach wykonawczych;

b) stosuje standardy i wytyczne dotyczące bezpieczeństwa w zakresie bezpieczeństwa osobowego, bezpieczeństwa fizycznego, zarządzania EUCI i bezpieczeństwa systemów teleinformatycznych (CIS), które zapewniają poziom ochrony EUCI równoważny poziomowi, jaki jest zapewniony w obrębie Komisji;

c) oznacza wytworzone przez siebie informacje niejawne jako EUCI.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, w ścisłej współpracy z innymi właściwymi departamentami Komisji, stanowi w obrębie Komisji służbę odpowiedzialną za zawieranie porozumień administracyjnych dotyczących wymiany EUCI z innymi instytucjami, agencjami, organami lub biurami UE.

3. Porozumienia administracyjne z reguły przyjmują formę wymiany listów podpisanych w imieniu Komisji przez Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa.

4. Przed zawarciem porozumienia administracyjnego dotyczącego wymiany EUCI organ ds. bezpieczeństwa Komisji przeprowadza wizytę oceniającą mającą na celu ocenę ram prawnych służących ochronie EUCI i upewnienie się co do skuteczności środków wdrożonych w celu ochrony EUCI. Porozumienie administracyjne wchodzi w życie i wymiana EUCI może się odbyć pod warunkiem że wynik wizyty oceniającej jest zadowalający, a zalecenia sformułowane po wizycie zostały spełnione. W regularnych odstępach czasu przeprowadza się kolejne wizyty oceniające mające na celu weryfikację zgodności z porozumieniem administracyjnym oraz zgodności obowiązujących środków bezpieczeństwa z uzgodnionymi podstawowymi zasadami i minimalnymi standardami.

5. W obrębie Komisji głównym punktem, do którego wpływają i z którego przekazywane są informacje niejawne wymieniane z inną instytucją, agencją, organem lub biurem UE, jest z reguły kancelaria tajna UE zarządzana przez Sekretariat Generalny. Jeżeli jednak ze względów bezpieczeństwa, organizacyjnych lub operacyjnych jest to dla ochrony EUCI właściwsze, jako punkt, do którego wpływają i z którego przekazywane są informacje niejawne dotyczące spraw wchodzących w zakres kompetencji danych departamentów Komisji, funkcjonują lokalne kancelarie tajne UE ustanowione w departamentach Komisji zgodnie z niniejsza decyzją i jej przepisami wykonawczymi.

6. O procesie zawierania porozumień administracyjnych zgodnie z ust. 2 informuje się Grupę Ekspertów ds. Bezpieczeństwa Komisji.

Artykuł 53

Wymiana EUCI z państwami członkowskimi

1. EUCI mogą być wymieniane z państwami członkowskimi oraz im udostępniane, pod warunkiem że państwa te chronią informacje zgodnie z wymogami mającymi zastosowanie w przypadku informacji niejawnych, którym nadano krajową klauzulę tajności o równorzędnym poziomie zgodnie z tabelą odpowiedników klauzul tajności zamieszczoną w załączniku I.

2. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci Unii Europejskiej informacje niejawne noszące krajowe oznaczenie identyfikujące dokument niejawny, Komisja obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI, na poziomie równorzędnym określonym w tabeli odpowiedników klauzul tajności zamieszczonej w załączniku I.

Artykuł 54

Wymiana EUCI z państwami trzecimi i organizacjami międzynarodowymi

1. W przypadku gdy Komisja stwierdza, że istnieje długoterminowa potrzeba wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową, podejmuje się niezbędne kroki w celu ustanowienia odpowiednich ram prawnych lub administracyjnych takiej wymiany, do których należeć mogą umowy o bezpieczeństwie informacji lub porozumienia administracyjne zawarte zgodnie z odpowiednimi przepisami.

2. Przedmiotowe umowy o bezpieczeństwie informacji i porozumienia administracyjne, o których mowa w ust. 1, zawierają postanowienia zapewniające, by w przypadku otrzymania EUCI przez państwa trzecie lub organizacje międzynarodowe informacje te były chronione stosownie do ich klauzuli tajności i zgodnie z minimalnymi standardami, które odpowiadają standardom określonym w niniejszej decyzji.

3. Komisja może zawierać porozumienia administracyjne zgodnie z art. 56, o ile poziom klauzuli tajności nadanej EUCI nie jest zasadniczo wyższy niż RESTREINT UE/EU RESTRICTED.

4. Porozumienia administracyjne dotyczące wymiany informacji niejawnych, o których mowa w ust. 3, zawierają postanowienia mające służyć temu, by w przypadku otrzymania EUCI przez państwa trzecie lub organizacje międzynarodowe informacje te były chronione stosownie do ich klauzuli tajności i zgodnie z minimalnymi standardami, które odpowiadają standardom określonym w niniejszej decyzji. W sprawie zawierania umów o bezpieczeństwie informacji lub porozumień administracyjnych zasięga się opinii Grupy Ekspertów ds. Bezpieczeństwa Komisji.

5. Decyzja o udostępnieniu państwu trzeciemu lub organizacji międzynarodowej EUCI wytworzonych w Komisji podejmowana jest przez departament Komisji, jako wytwórcę przedmiotowych EUCI w obrębie Komisji, dla każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, potrzeby odbiorcy w zakresie dostępu do informacji niejawnych i korzyści dla Unii. Jeżeli wytwórcą informacji niejawnych, o których udostępnienie wystąpiono, lub materiału źródłowego, który mogą zawierać, nie jest Komisja, departament Komisji, który posiada przedmiotowe informacje niejawne, najpierw zwraca się do wytwórcy o pisemną zgodę na ich udostępnienie. Jeżeli nie można ustalić, kto jest wytwórcą, departament Komisji, który posiada przedmiotowe informacje niejawne, przejmuje odpowiedzialność wytwórcy po uprzedniej konsultacji z Grupą Ekspertów ds. Bezpieczeństwa Komisji.

Artykuł 55

Umowy o bezpieczeństwie informacji

1. Umowy o bezpieczeństwie informacji zawierane są między państwami trzecimi lub organizacjami międzynarodowymi zgodnie z art. 218 TFUE.

2. Umowy o bezpieczeństwie informacji:

a) ustanawiają podstawowe zasady i minimalne standardy mające zastosowanie do wymiany informacji niejawnych między Unią a państwem trzecim lub organizacją międzynarodową;

b) przewidują techniczne uzgodnienia wykonawcze, dokonywane przez właściwe organy bezpieczeństwa odpowiednich instytucji i organów Unii oraz właściwy organ bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej. Przedmiotowe uzgodnienia uwzględniają poziom ochrony przewidziany w przepisach, strukturach i procedurach dotyczących bezpieczeństwa istniejących w danym państwie trzecim lub danej organizacji międzynarodowej;

c) przewidują, że przed wymianą informacji niejawnych na mocy umowy należy upewnić się, że strona otrzymująca jest w stanie w odpowiedni sposób chronić i zabezpieczać dostarczone jej informacje niejawne.

3. Jeżeli ustalono potrzebę wymiany informacji niejawnych zgodnie z art. 51 ust. 1, Komisja konsultuje się z Europejską Służbą Działań Zewnętrznych, Sekretariatem Generalnym Rady oraz innymi instytucjami i organami UE, w razie potrzeby, w celu ustalenia, czy należy złożyć zalecenie w myśl art. 218 ust. 3 TFUE.

4. Nie wymienia się żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w umowie o bezpieczeństwie informacji lub technicznych uzgodnieniach wykonawczych.

5. Główny punkt w obrębie Komisji, do którego wpływają i z którego przekazywane są informacje niejawne wymieniane z państwami trzecimi i organizacjami międzynarodowymi, stanowi z reguły kancelaria tajna UE zarządzana przez Sekretariat Generalny. Jeżeli jednak ze względów bezpieczeństwa, organizacyjnych lub operacyjnych jest to dla ochrony EUCI właściwsze, jako punkt, do którego wpływają i z którego przekazywane są informacje niejawne dotyczące spraw wchodzących w zakres kompetencji danych departamentów Komisji, funkcjonują lokalne kancelarie tajne UE ustanowione w departamentach Komisji zgodnie z niniejsza decyzją i jej przepisami wykonawczymi.

6. Aby ocenić skuteczność przepisów, struktur i procedur dotyczących bezpieczeństwa w danym państwie trzecim lub organizacji międzynarodowej, Komisja – w porozumieniu z zainteresowanym państwem trzecim lub organizacją międzynarodową oraz we współpracy z innymi instytucjami, agencjami, organami lub biurami UE – uczestniczy w wizytach oceniających. Takie wizyty oceniające służą ewaluacji:

a) ram prawnych mających zastosowanie do ochrony informacji niejawnych;

b) wszelkich cech charakterystycznych polityki bezpieczeństwa oraz sposobu, w jaki zorganizowana jest polityka bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, co może mieć wpływ na poziom tajności informacji niejawnych, które mogą być wymieniane;

c) stosowanych faktycznie środków i procedur bezpieczeństwa; oraz

d) procedur sprawdzających w zakresie poświadczenia bezpieczeństwa odpowiadających klauzuli tajności EUCI, które mają być udostępniane.

Artykuł 56

Porozumienia administracyjne

1. Jeżeli w kontekście ram politycznych lub prawnych UE istnieje długoterminowa potrzeba wymiany z państwem trzecim lub organizacją międzynarodową informacji niejawnych z klauzulą tajności z reguły nie wyższą niż RESTREINT UE/EU RESTRICTED i jeżeli organ ds. bezpieczeństwa Komisji po konsultacji z Grupą Ekspertów ds. Bezpieczeństwa Komisji ustalił w szczególności, że dana strona nie dysponuje wystarczająco rozwiniętym systemem bezpieczeństwa, aby można było zawrzeć umowę o bezpieczeństwie informacji, Komisja może zadecydować o zawarciu porozumienia administracyjnego z odpowiednimi organami danego państwa trzeciego lub organizacji międzynarodowej.

2. Przedmiotowe porozumienia administracyjne co do zasady przyjmują postać wymiany listów.

3. Przed zawarciem porozumienia przeprowadza się wizytę oceniającą. O wyniku takiej wizyty informuje się Grupę Ekspertów ds. Bezpieczeństwa Komisji. Jeżeli istnieją wyjątkowe powody dla pilnej wymiany informacji niejawnych, EUCI mogą być udostępniane pod warunkiem że dołoży się wszelkich starań, aby przedmiotowa wizyta oceniająca została przeprowadzona jak najszybciej.

4. Nie wymienia się żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w porozumieniu administracyjnym.

Artykuł 57

Wyjątkowe udostępnianie EUCI *ad hoc*

1. Jeżeli nie zawarto umowy o bezpieczeństwie informacji lub porozumienia administracyjnego, a Komisja lub jeden z jej departamentów stwierdzi, że w kontekście ram politycznych i prawnych UE istnieje wyjątkowa potrzeba udostępnienia EUCI państwu trzeciemu lub organizacji międzynarodowej, organ ds. bezpieczeństwa Komisji sprawdza – w możliwie obszernym zakresie – wraz z organami bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej, czy ich przepisy, struktury i procedury dotyczące bezpieczeństwa gwarantują ochronę udostępnianych EUCI zgodnie ze standardami, które nie są mniej rygorystyczne niż standardy określone w niniejszej decyzji.

2. Decyzja udostępnienia EUCI danemu państwu trzeciemu lub organizacji międzynarodowej podejmowana jest, po konsultacji z Grupą Ekspertów ds. Bezpieczeństwa Komisji, przez Komisję na podstawie wniosku członka Komisji odpowiedzialnego za kwestie bezpieczeństwa.

3. W następstwie decyzji Komisji o udostępnieniu EUCI i po uprzednim uzyskaniu pisemnej zgody wytwórców, w tym wytwórców materiału źródłowego, który informacje mogą zawierać, właściwy departament Komisji przekazuje przedmiotowe informacje, które są opatrzone oznaczeniem dotyczącym możliwości ich udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym zostają udostępnione. Przed faktycznym udostępnieniem lub w momencie udostępniania dana strona trzecia na piśmie zobowiązuje się do ochrony EUCI, które otrzymuje, zgodnie z podstawowymi zasadami i minimalnymi standardami określonymi w niniejszej decyzji.

ROZDZIAŁ 8

PRZEPISY KOŃCOWE

Artykuł 58

Zastąpienie poprzedniej decyzji

Niniejsza decyzja uchyla i zastępuje decyzję Komisji 2001/844/WE, EWWiS, Euratom ([1]).

Artykuł 59

Informacje niejawne wytworzone przed wejściem w życie niniejszej decyzji

1. Wszystkie EUCI opatrzone klauzulą tajności zgodnie z decyzją 2001/844/WE, EWWiS, Euratom podlegają dalszej ochronie zgodnie z właściwymi przepisami niniejszej decyzji.

2. W dniu wejścia w życie niniejszej decyzji 2001/844/WE, EWWiS, Euratom wszystkie informacje niejawne, które uprzednio znalazły się w Komisji, z wyłączeniem informacji niejawnych Euratom:

a) jeśli zostały wytworzone przez Komisję, w dalszym ciągu są uznawane za automatycznie przeklasyfikowane na „RESTREINT UE", chyba że ich autor podjął do dnia 31 stycznia 2002 r. decyzję o nadaniu im innej klauzuli i poinformował o tym wszystkich adresatów danego dokumentu;

b) jeśli zostały wytworzone przez autorów spoza Komisji, zachowują oryginalną klauzulę tajności i tym samym są traktowane jak EUCI z równorzędną klauzulą, chyba że autor wyraził zgodę na jej obniżenie lub zniesienie.

Artykuł 60

Przepisy wykonawcze i instrukcje bezpieczeństwa

1. W stosownych przypadkach przyjęcie przepisów wykonawczych do niniejszej decyzji będzie przedmiotem odrębnej decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa, w pełnej zgodności z regulaminem wewnętrznym.

2. Po uzyskaniu uprawnień w następstwie wyżej wspomnianej decyzji Komisji członek Komisji odpowiedzialny za kwestie bezpieczeństwa może opracować instrukcje bezpieczeństwa, w których określi wytyczne dotyczące bezpieczeństwa i najlepsze praktyki w zakresie niniejszej decyzji i jej przepisów wykonawczych.

3. Komisja może przekazać zadania wspomniane w ust. 1 i 2 niniejszego artykułu Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa w ramach osobnej decyzji w sprawie przekazywania zadań, w pełnej zgodności z regulaminem wewnętrznym.

Artykuł 61

Wejście w życie

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

Sporządzono w Brukseli dnia 13 marca 2015 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

([1]) Decyzja Komisji 2001/844/WE, EWWiS, Euratom z dnia 29 listopada 2001 r. zmieniająca jej regulamin wewnętrzny (Dz.U. L 317 z 3.12.2001, s. 1).

ZAŁĄCZNIK I

ODPOWIEDNIKI KLAUZUL TAJNOŚCI

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET,	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED,
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	uwaga ([1]) poniżej
Bułgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Republika Czeska	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dania	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Niemcy	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlandia	Top Secret	Secret	Confidential	Restricted
Grecja	Άκρως Απόρρητο Skrót: ΑΑΠ	Απόρρητο Skrót: (ΑΠ)	Εμπιστευτικό Skrót: (ΕΜ)	Περιορισμένης Χρήσης Skrót: (ΠΧ)
Hiszpania	Secreto	Reservado	Confidencial	Difusión Limitada
Francja	Très Secret Défense	Secret Défense	Confidentiel Défense	uwaga ([3]) poniżej
Chorwacja	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Cypr	Άκρως Απόρρητο Skrót: (ΑΑΠ)	Απόρρητο Skrót: (ΑΠ)	Εμπιστευτικό Skrót: (ΕΜ)	Περιορισμένης Χρήσης Skrót: (ΠΧ)
Łotwa	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litwa	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luksemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Węgry	„Szigorúan titkos!”	„Titkos!”	„Bizalmas!”	„Korlátozott terjesztésű!”
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Niderlandy	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polska	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET,	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED,
Rumunia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Słowenia	Strogo tajno	Tajno	Zaupno	Interno
Słowacja	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Szwecja ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Zjednoczone Królestwo	UK TOP SECRET	UK SECRET	Brak odpowiednika ([5])	UK OFFICIAL – SENSITIVE

([1]) Oznaczenie Restreinte/Beperkte Verspreiding nie jest w Belgii uznawane za klauzulę tajności. W Belgii pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE/EU RESTRICTED" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to normy i procedury opisane w przepisach bezpieczeństwa Rady Unii Europejskiej.

([2]) Niemcy: VS = Verschlusssache.

([3]) Francja nie stosuje klauzuli „RESTREINT" w swoim systemie krajowym. We Francji pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE/EU RESTRICTED" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to standardy i procedury opisane w przepisach bezpieczeństwa Rady Unii Europejskiej.

([4]) Szwecja: oznaczenia klauzuli tajności w górnym rzędzie są używane przez organy obrony, zaś oznaczenia w dolnym rzędzie — przez inne organy.

([5]) W Zjednoczonym Królestwie pracuje się z wykorzystaniem EUCI oznaczonych CONFIDENTIEL UE/EU CONFIDENTIAL i chroni je zgodnie z wymaganiami bezpieczeństwa dla informacji oznaczonych UK SECRET.

ZAŁĄCZNIK II

WYKAZ SKRÓTÓW

Akronim	Znaczenie
CA	Organ ds. kryptograficznych
CAA	Organ ds. zatwierdzania produktów kryptograficznych
CCTV	Telewizja przemysłowa
CDA	Organ ds. dystrybucji produktów kryptograficznych
CIS	Systemy teleinformatyczne, w których przetwarzane są EUCI
WWB	Wyznaczona władza bezpieczeństwa
EUCI	Informacje niejawne UE
SBP	Świadectwo bezpieczeństwa przemysłowego
ZI	Zabezpieczanie informacji
OZI	Organ ds. zabezpieczania informacji
SSWiN	System sygnalizacji włamania i napadu
IT	Technologia informacyjna
LPO	Lokalny pełnomocnik ochrony
KWB	Krajowa władza bezpieczeństwa
PBO	Poświadczenie bezpieczeństwa osobowego
ZPBO	Zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego
IBP	Instrukcje bezpieczeństwa programu lub projektu
KKT	Kierownik kancelarii tajnej
OAB	Organ ds. akredytacji bezpieczeństwa
DOAB	Dokument określający aspekty bezpieczeństwa
PNK	Przewodnik nadawania klauzul
PBES	Procedura bezpiecznej eksploatacji systemu
TA	Organ ds. TEMPEST
TFUE	Traktat o funkcjonowaniu UE

ZAŁĄCZNIK III

WYKAZ KRAJOWYCH WŁADZ BEZPIECZEŃSTWA

BELGIA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. sekretariatu: +32 25014542
Faks: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BUŁGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Faks: +359 29873750
E-mail: dksi@government.bg
Strona internetowa: www.dksi.bg

REPUBLIKA CZESKA

Národní bezpečnostní úřad
(Krajowa władza bezpieczeństwa)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Faks: +420 257283110
E-mail: czech.nsa@nbu.cz
Strona internetowa: www.nbu.cz

DANIA

Politiets Efterretningstjeneste
(Duńska Służba Wywiadowcza ds. Bezpieczeństwa)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Faks: +45 33430190

Forsvarets Efterretningstjeneste
(Duńska Służba Wywiadowcza ds. Obrony)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Faks: +45 33931320

NIEMCY

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Tel. +49 30186810
Faks: +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIA

Departament ds. Bezpieczeństwa Narodowego
Estońskie Ministerstwo Obrony
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Faks: +372 7170213
E-mail: nsa@mod.gov.ee

GRECJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Sztab Generalny Obrony Narodowej Grecji (HNDGS)
Dyrekcja Sektor Wywiadu Wojskowego
Dyrekcja Kontrwywiad na rzecz Bezpieczeństwa
GR-STG 1020 Holargos – Ateny
Tel. +30 2106572045
+ 30 2106572009
Faks: +30 2106536279, +30 2106577612

HISZPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Faks: +34 913725808
E-mail: nsa-sp@areatec.com

FRANCJA

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07SP
Tel. +33 171758177
Faks: + 33 171758200

CHORWACJA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Chorwacja
Tel. +385 14681222
Faks: + 385 14686049
Strona internetowa: www.uvns.hr

IRLANDIA

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Faks: +353 14082959

WŁOCHY

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel. +39 0661174266
Faks: +39 064885273

CYPR

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+357 22807764
Faks: +357 22302351
E-mail: cynsa@mod.gov.cy

ŁOTWA

Krajowa władza bezpieczeństwa
Biuro Ochrony Konstytucji Republiki Łotwy
P.O.Box 286
LV-1001 Rīga
Tel. +371 67025418
Faks: +371 67025454
E-mail: ndi@sab.gov.lv

LITWA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Komisja Koordynacji Ochrony Informacji Niejawnych Republiki Litwy Krajowa Władza Bezpieczeństwa)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Faks: +370 706 66700
E-mail: nsa@vsd.lt

LUKSEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luksemburg
Tel. +352 24782210 (centrala)
+ 352 24782253 (bezpośredni)
Faks: +352 24782243

WĘGRY

Nemzeti Biztonsági Felügyelet
(Krajowa władza bezpieczeństwa Węgier)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Faks: +36 (1) 7950344

Adres pocztowy:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Strona internetowa: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Faks: +356 25695321

NIDERLANDY

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Faks: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Faks: +31 703187522

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Faks: +43 1531152615
E-mail: ISK@bka.gv.at

POLSKA

Agencja Bezpieczeństwa Wewnętrznego – ABW
ul. Rakowiecka 2A
00-993 Warszawa
Tel. +48 225857944
faks: +48 225857443
E-mail: nsa@abw.gov.pl
Strona internetowa: www.abw.gov.pl

PORTUGALIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Faks: +351 213031711

RUMUNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Rumuńska krajowa władza bezpieczeństwa – ORNISS Urząd państwowego rejestru informacji niejawnych)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Faks: +40 212240714
E-mail: nsa.romania@nsa.ro
Strona internetowa: www.orniss.ro

SŁOWENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Faks: +386 14781399
E-mail: gp.uvtp@gov.si

SŁOWACJA

Národný bezpečnostný úrad
(Krajowa władza bezpieczeństwa)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Faks: +421 263824005
Strona internetowa: www.nbusr.sk

FINLANDIA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Faks: +358 916055140
E-mail: NSA@formin.fi

SZWECJA

Utrikesdepartementet
(Ministerstwo Spraw Zagranicznych)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Faks: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

ZJEDNOCZONE KRÓLESTWO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Faks: +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

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

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL