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