II

(Akty o charakterze nieustawodawczym)

DECYZJE

DECYZJA RADY

z dnia 31 marca 2011 r.

w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE

(2011/292/UE)

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 240 ust. 3,

uwzględniając decyzję Rady 2009/937/UE z dnia 1 grudnia 2009 r. dotyczącą przyjęcia regulaminu wewnętrznego Rady [1], w szczególności jej art. 24,

a także mając na uwadze, co następuje:

(1) Aby rozwinąć działania Rady we wszystkich dziedzinach wymagających wykorzystywania informacji niejawnych, właściwe jest utworzenie kompleksowego systemu bezpieczeństwa służącego ochronie informacji niejawnych, który obejmie Radę, jej Sekretariat Generalny oraz państwa członkowskie.

(2) Niniejsza decyzja powinna mieć zastosowanie do przypadków, gdy Rada, jej organy przygotowawcze oraz Sekretariat Generalny Rady (SGR) wykorzystują informacje niejawne UE (EUCI).

(3) Zgodnie z krajowymi przepisami ustawowymi i wykonawczymi i w zakresie, jaki jest niezbędny do funkcjonowania Rady, w przypadkach gdy właściwe organy, pracownicy lub wykonawcy z państw członkowskich wykorzystują EUCI, państwa członkowskie powinny przestrzegać niniejszej decyzji, tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony EUCI.

(4) Rada i Komisja są zdecydowane stosować równoważne normy bezpieczeństwa w celu ochrony EUCI.

(5) Rada podkreśla znaczenie włączania się, w odpowiednich przypadkach, Parlamentu Europejskiego i innych instytucji, agencji, organów lub biur UE w przestrzeganie zasad, norm i przepisów dotyczących ochrony informacji niejawnych, które są niezbędne do ochrony interesów Unii i jej państw członkowskich.

(6) Agencje i organy UE utworzone na mocy tytułu V rozdział 2 Traktatu o Unii Europejskiej, Europol i Eurojust stosują w ramach swoich struktur wewnętrznych podstawowe zasady i minimalne normy określone w niniejszej decyzji w celu ochrony EUCI, zgodnie z tym, co przewidują akty założycielskie tych agencji i organów.

(7) Do operacji zarządzania kryzysowego organizowanych na mocy tytułu V rozdział 2 TUE oraz do personelu biorącego w nich udział stosuje się przepisy bezpieczeństwa przyjęte przez Radę w celu ochrony EUCI.

(8) Specjalni przedstawiciele UE i członkowie ich zespołów stosują przepisy bezpieczeństwa przyjęte przez Radę w celu ochrony EUCI.

(9) Niniejsza decyzja zostaje przyjęta bez uszczerbku dla art. 15 i 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz aktów prawnych służących wykonaniu tych artykułów.

(10) Niniejsza decyzja zostaje przyjęta bez uszczerbku dla istniejących w państwach członkowskich praktyk w zakresie powiadamiania parlamentów krajowych o działaniach Unii,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Cel, zakres stosowania i definicje

1. Niniejsza decyzja określa podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie EUCI.

[1] Dz.U. L 325 z 11.12.2009, s. 35.

2. Te podstawowe zasady i minimalne normy bezpieczeństwa mają zastosowanie do Rady i SGR oraz przestrzegane są przez państwa członkowskie zgodnie z ich krajowymi przepisami ustawowymi i wykonawczymi, tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony EUCI.

3. Do celów niniejszej decyzji zastosowanie mają definicje zamieszczone w dodatku A.

Artykuł 2

Definicja EUCI, klauzule tajności i oznaczenia

1. „Informacje niejawne UE" (EUCI) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego.

2. EUCI otrzymują jedną z następujących klauzul tajności:

a) TRÈS 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 nadaje się klauzulę tajności zgodnie z ust. 2. Można nadać im dodatkowe oznaczenie wskazujące na dziedzinę działalności, do której się odnoszą, na wytwórcę, ograniczenia dystrybucji, ograniczenia wykorzystania lub możliwość ujawnienia.

Artykuł 3

Oznaczanie klauzulami tajności

1. Właściwe organy zapewniają, by EUCI nadawano odpowiednie klauzule tajności, by informacje takie były wyraźnie oznaczone jako informacje niejawne, a także by były one objęte danym poziomem klauzuli tajności nie dłużej, niż jest to konieczne.

2. Do obniżenia lub zniesienia klauzuli tajności nadanej EUCI oraz do zmiany lub usunięcia oznaczeń, o których mowa w art. 2 ust. 3, potrzebna jest uprzednia pisemna zgoda wytwórcy.

3. Rada zatwierdza politykę bezpieczeństwa w zakresie wytwarzania EUCI, która obejmuje praktyczny przewodnik nadawania klauzul tajności.

Artykuł 4

Ochrona informacji niejawnych

1. EUCI są chronione zgodnie z niniejszą decyzją.

2. Posiadacz jakichkolwiek EUCI jest odpowiedzialny za ich ochronę zgodnie z niniejszą decyzją.

3. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci Unii Europejskiej informacje niejawne, którym nadano krajową klauzulę tajności, Rada i SGR obejmują te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI mających równorzędną klauzulę tajności – zgodnie z tabelą odpowiedników klauzul tajności zamieszczoną w dodatku B.

4. Uzasadnione może być objęcie dużych ilości lub kompilacji EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności.

Artykuł 5

Zarządzanie ryzykiem dla bezpieczeństwa

1. Zarządzanie ryzykiem naruszenia EUCI przebiega w ramach określonego procesu. Proces ten jest ukierunkowany na określenie rodzajów ryzyka naruszenia zasad bezpieczeństwa, środków bezpieczeństwa służących zmniejszeniu tego ryzyka do akceptowalnego poziomu zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa przedstawionymi w niniejszej decyzji oraz na zastosowanie tych środków zgodnie z koncepcją ochrony w głąb, zdefiniowaną w dodatku A. Skuteczność takich środków jest stale poddawana ocenie.

2. 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 zagrożenia wystąpieniem w tym miejscu działań realizowanych w złych zamiarach lub działalności przestępczej, takiej jak działalność szpiegowska, sabotażowa lub terrorystyczna.

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

4. W planach ciągłości działania zamieszczane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z wykorzystywaniem EUCI oraz z ich przechowywaniem.

Artykuł 6

Wprowadzenie w życie niniejszej decyzji

1. Jeżeli to konieczne, Rada na zalecenie Komitetu ds. Bezpieczeństwa zatwierdza polityki bezpieczeństwa przewidujące środki służące wprowadzeniu w życie niniejszej decyzji.

2. Komitet ds. Bezpieczeństwa może na swoim poziomie uzgodnić wytyczne dotyczące bezpieczeństwa, które będą uzupełniać lub wspierać niniejszą decyzję i wszelkie polityki bezpieczeństwa zatwierdzone przez Radę.

Artykuł 7

Bezpieczeństwo osobowe

1. Bezpieczeństwo osobowe oznacza stosowanie środków gwarantujących, że dostęp do EUCI jest przyznawany tylko osobom, które:

— spełniają zasadę ograniczonego dostępu,

— w odpowiednich przypadkach zostały odpowiednio sprawdzone, oraz

— zostały poinformowane o swoich obowiązkach.

2. Procedury prowadzenia postępowań sprawdzających mają na celu stwierdzenie, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnić do dostępu do EUCI.

3. Wszystkie osoby pracujące w SGR, których obowiązki mogą wymagać dostępu do EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, są przed uzyskaniem dostępu do takich EUCI odpowiednio sprawdzane. Procedura prowadzenia postępowań sprawdzających dotyczących urzędników i innych pracowników SGR przedstawiona jest w załączniku I.

4. Pracownicy państw członkowskich, o których mowa w art. 14 ust. 3, których obowiązki mogą wymagać dostępu do EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, są przed uzyskaniem dostępu do takich EUCI odpowiednio sprawdzani lub otrzymują inne odpowiednie upoważnienie ze względu na pełnione przez siebie funkcje, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

5. Przed uzyskaniem dostępu do EUCI, a następnie w regularnych odstępach czasu wszystkie osoby informowane są o obowiązku ochrony tych informacji zgodnie z niniejszą decyzją i potwierdzają znajomość tego obowiązku.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku I.

Artykuł 8

Bezpieczeństwo fizyczne

1. Bezpieczeństwo fizyczne oznacza stosowanie fizycznych i technicznych środków ochrony, aby zapobiec nieuprawnionemu dostępowi do EUCI.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie 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 dostępu do EUCI zgodnie z zasadą ograniczonego dostępu. Środki te określane są na podstawie procesu zarządzania ryzykiem.

3. Środkami bezpieczeństwa fizycznego obejmuje się wszystkie obiekty, budynki, biura, pomieszczenia i inne strefy, w których są wykorzystywane lub przechowywane EUCI, w tym strefy, w których znajdują się systemy teleinformatyczne określone w art. 10 ust. 2.

4. Strefy, w których przechowywane są EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, ustanawiane są strefami bezpieczeństwa zgodnie z załącznikiem II; strefy takie zatwierdza właściwy organ bezpieczeństwa.

5. Do ochrony EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej stosuje się wyłącznie zatwierdzony sprzęt lub zatwierdzone urządzenia.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku II.

Artykuł 9

Zarządzanie informacjami niejawnymi

1. Zarządzanie informacjami niejawnymi polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w art. 7, 8 i 10, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa tych informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przewożenia i niszczenia EUCI.

2. Informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Właściwe organy SGR i państw członkowskich ustanawiają do tego celu system kancelarii tajnych. Informacje niejawne o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.

3. Jednostki organizacyjne i obiekty, w których są wykorzystywane lub przechowywane EUCI, poddawane są regularnym inspekcjom przeprowadzanym przez właściwy organ bezpieczeństwa.

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

a) z reguły EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 10 ust. 6;

b) gdy sposób, o którym mowa w lit. a) nie jest wykorzystywany, EUCI są przekazywane:

(i) za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 10 ust. 6; albo

(ii) we wszystkich pozostałych przypadkach, zgodnie z wytycznymi właściwego organu bezpieczeństwa wydanymi w myśl odpowiednich środków ochrony określonych w załączniku III.

5. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku III.

Artykuł 10

Ochrona EUCI przetwarzanych w systemach teleinformatycznych

1. Zabezpieczanie informacji w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, które są przez nie przetwarzane, i będą działać zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.

2. „System teleinformatyczny" oznacza system umożliwiający przetwarzanie informacji w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne. Niniejsza decyzja ma zastosowanie do systemów teleinformatycznych przetwarzających EUCI (CIS).

3. CIS przetwarza EUCI zgodnie z koncepcją zabezpieczania informacji.

4. Wszystkie CIS poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony EUCI i CIS zgodnie z niniejszą decyzją. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, które mogą być przetwarzane w ramach danego CIS, oraz odpowiednie warunki.

5. CIS przetwarzające informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej są chronione w taki sposób, by bezpieczeństwo informacji nie mogło zostać narażone na szwank z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST").

6. Jeżeli EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane w sposób następujący:

a) poufność informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET i wyższej podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez Radę działającą jako organ ds. zatwierdzania produktów kryptograficznych (CAA);

b) poufność informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub RESTREINT UE/EU RESTRICTED podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez Sekretarza Generalnego Rady (zwanego dalej „Sekretarzem Generalnym") działającego jako CAA.

Niezależnie od przepisów lit. b) w obrębie krajowych systemów państw członkowskich poufność EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub RESTREINT UE/EU RESTRICTED może być chroniona przy użyciu produktów kryptograficznych zatwierdzonych przez CAA danego państwa członkowskiego.

7. Podczas transmisji EUCI drogą elektroniczną stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w wyjątkowych okolicznościach mogą mieć zastosowanie szczególne procedury lub szczególne konfiguracje techniczne określone w załączniku IV.

8. Właściwe organy, odpowiednio, SGR i państw członkowskich ustanawiają następujące organy zajmujące się zabezpieczaniem informacji:

a) organ ds. zabezpieczania informacji (IAA);

b) organ ds. TEMPEST (TA);

c) organ ds. zatwierdzania produktów kryptograficznych (CAA);

d) organ ds. dystrybucji produktów kryptograficznych (CDA).

9. W odniesieniu do każdego systemu właściwe organy, odpowiednio, SGR i państw członkowskich ustanawiają:

a) organ ds. akredytacji bezpieczeństwa (SAA);

b) organ operacyjny ds. zabezpieczania informacji.

10. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku IV.

Artykuł 11

Bezpieczeństwo przemysłowe

1. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Umowy takie nie obejmują dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET.

2. SGR może na podstawie umowy powierzyć zadania obejmujące EUCI lub wiążące się z dostępem do tych informacji, ich wykorzystywaniem lub przechowywaniem przez podmioty prowadzące działalność gospodarczą lub inną, zarejestrowane w państwie członkowskim lub w państwie trzecim, które zawarło umowę lub porozumienie administracyjne zgodnie z art. 12 ust. 2 lit. a) lub b).

3. Jako instytucja zamawiająca SGR zapewnia, by w przypadku zawierania umów niejawnych z podmiotami prowadzącymi działalność gospodarczą lub inną spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie.

4. Krajowa władza bezpieczeństwa (KWB), wyznaczona władza bezpieczeństwa (WWB) lub jakikolwiek inny właściwy organ bezpieczeństwa każdego państwa członkowskiego zapewniają – w zakresie, jaki umożliwiają to krajowe przepisy ustawowe i wykonawcze – by wykonawcy i podwykonawcy zarejestrowani na ich terytorium stosowali wszelkie odpowiednie środki mające chronić EUCI podczas negocjacji poprzedzających zawarcie umowy i podczas wykonywania umowy niejawnej.

5. KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa każdego państwa członkowskiego zapewniają, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, by wykonawcy lub podwykonawcy zarejestrowani w tym państwie członkowskim, będący stronami umów niejawnych lub niejawnych umów o podwykonawstwo i którym niezbędny jest dostęp w ich obiektach do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET podczas wykonywania takich umów lub na etapie poprzedzającym ich zawarcie, posiadali świadectwo bezpieczeństwa przemysłowego (SBP) do odpowiedniego poziomu klauzuli tajności.

6. Odpowiednia KWB, WWB lub jakikolwiek inny właściwy organ bezpieczeństwa wydaje pracownikom wykonawcy lub podwykonawcy, którym przy wykonywaniu umowy niejawnej niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, poświadczenie bezpieczeństwa osobowego (PBO) zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku I.

7. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku V.

Artykuł 12

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

1. Jeżeli Rada stwierdza, że zachodzi konieczność wymiany EUCI z państwem trzecim lub organizacją międzynarodową, ustanowione zostają odpowiednie ramy takiej wymiany.

2. Aby ustanowić takie ramy i określić wzajemnie obowiązujące zasady ochrony wymienianych informacji niejawnych,

a) Rada zawiera umowy dotyczące procedur bezpieczeństwa na potrzeby wymiany i ochrony informacji niejawnych (zwane dalej „umowami o bezpieczeństwie informacji"); lub

b) Sekretarz Generalny może zgodnie z pkt 17 załącznika VI zawierać porozumienia administracyjne, o ile poziom klauzuli tajności nadanej EUCI, które mają zostać udostępnione, nie jest – co do zasady – wyższy niż RESTREINT UE/EU RESTRICTED.

3. Umowy o bezpieczeństwie informacji lub porozumienia administracyjne, o których mowa w ust. 2, zawierają postanowienia mające służyć temu, by w przypadku gdy państwa trzecie lub organizacje międzynarodowe otrzymają EUCI, informacje te były chronione w sposób odpowiadający ich klauzuli tajności i zgodny z minimalnymi normami, które nie mogą być mniej rygorystyczne niż normy określone w niniejszej decyzji.

4. Decyzja o udostępnieniu państwu trzeciemu lub organizacji międzynarodowej EUCI wytworzonych w Radzie podejmowana jest przez Radę po rozpatrzeniu każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, od tego, czy odbiorca spełnia zasadę ograniczonego dostępu, i od tego, w jakim stopniu jest to korzystne dla UE. Jeżeli wytwórcą informacji niejawnych, o których udostępnienie wystąpiono, nie jest Rada, SGR najpierw zwraca się o pisemną zgodę wytwórcy na ich udostępnienie. Jeżeli nie można ustalić, kto jest wytwórcą, Rada przejmuje jego odpowiedzialność.

5. Aby stwierdzić skuteczność środków bezpieczeństwa stosowanych w państwie trzecim lub organizacji międzynarodowej w celu ochrony EUCI, które zostały im przekazane jednostronnie lub w ramach wymiany, przeprowadzane są wizyty oceniające.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku VI.

Artykuł 13

Naruszenie i narażenie na szwank bezpieczeństwa EUCI

1. Naruszenie zasad bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania w sposób sprzeczny z zasadami bezpieczeństwa ustanowionymi w niniejszej decyzji.

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 wszelkich podejrzeniach lub przypadkach naruszenia zasad bezpieczeństwa powiadamia się niezwłocznie właściwy organ bezpieczeństwa.

4. Jeżeli wiadomo lub jeżeli istnieją uzasadnione przesłanki, by przypuszczać, że bezpieczeństwo EUCI zostało narażone na szwank lub że informacje takie zostały utracone, właściwy organ bezpieczeństwa podejmuje – zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi – wszelkie stosowne działania służące:

a) poinformowaniu wytwórcy informacji;

b) zapewnieniu zbadania tego przypadku przez personel niezwiązany bezpośrednio z tym naruszeniem w celu ustalenia przebiegu wydarzeń;

c) ocenie potencjalnych szkód dla interesów UE lub państw członkowskich;

d) podjęciu właściwych środków w celu zapobieżenia powtórzeniu się podobnego przypadku; oraz

e) powiadomieniu właściwych organów o podjętych działaniach.

5. Każda osoba odpowiedzialna za naruszenie przepisów dotyczących bezpieczeństwa określonych w niniejszej decyzji może podlegać postępowaniu dyscyplinarnemu zgodnie z mającymi zastosowanie zasadami i przepisami wykonawczymi. 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.

Artykuł 14

Odpowiedzialność za wprowadzenie decyzji w życie

1. Rada podejmuje wszelkie niezbędne działania w celu zapewnienia ogólnej spójności w stosowaniu niniejszej decyzji.

2. Sekretarz Generalny podejmuje wszelkie niezbędne działania w celu zapewnienia stosowania niniejszej decyzji przez urzędników i innych pracowników SGR, personel oddelegowany do SGR i wykonawców zatrudnionych przez SGR, przy wykorzystywaniu lub przechowywaniu EUCI lub jakichkolwiek innych informacji niejawnych, w obiektach, z których korzysta Rada, oraz w obrębie SGR, w tym w obrębie biur łącznikowych znajdujących się w państwach trzecich.

3. Państwa członkowskie podejmują – zgodnie ze swoimi przepisami ustawowymi i wykonawczymi – wszelkie stosowne działania w celu zapewnienia przestrzegania niniejszej decyzji, przy wykorzystywaniu lub przechowywaniu EUCI, przez:

a) pracowników stałych przedstawicielstw państw członkowskich przy Unii Europejskiej, a także delegatów krajowych uczestniczących w posiedzeniach Rady lub jej organów przygotowawczych lub biorących udział w innych działaniach Rady;

b) innych pracowników administracji krajowej państw członkowskich, w tym pracowników oddelegowanych do pracy w tej administracji, gdy pełnią oni obowiązki na terytorium państw członkowskich lub poza ich granicami;

c) inne osoby w państwach członkowskich, które ze względu na pełnione funkcje posiadają odpowiednie upoważnienie do dostępu do EUCI; oraz

d) wykonawców zatrudnionych przez państwa członkowskie na terytorium państw członkowskich lub poza ich granicami.

Artykuł 15

Organizacja bezpieczeństwa w Radzie

1. W ramach zapewniania ogólnej spójności w stosowaniu niniejszej decyzji Rada zatwierdza:

a) umowy, o których mowa w art. 12 ust. 2 lit. a);

b) decyzje zezwalające na udostępnienie EUCI państwom trzecim i organizacjom międzynarodowym;

c) roczny program inspekcji proponowany przez Sekretarza Generalnego i zalecany przez Komitet ds. Bezpieczeństwa; program ten dotyczy inspekcji jednostek organizacyjnych i obiektów w państwach członkowskich oraz inspekcji agencji i organów UE utworzonych na mocy tytułu V rozdział 2 TUE, jak również Europolu i Eurojustu, oraz wizyt oceniających przeprowadzanych w państwach trzecich i w organizacjach międzynarodowych w celu sprawdzenia skuteczności środków wprowadzonych, by chronić EUCI; oraz

d) polityki bezpieczeństwa przewidziane w art. 6 ust. 1.

2. Organem bezpieczeństwa SGR jest Sekretarz Generalny. Pełniąc tę funkcję, Sekretarz Generalny:

a) wdraża politykę bezpieczeństwa opracowaną przez Radę i dokonuje jej przeglądu;

b) koordynuje z KWB państw członkowskich wszystkie kwestie bezpieczeństwa dotyczące ochrony informacji niejawnych mających związek z działaniami Rady;

c) wydaje PBO UE urzędnikom i innym pracownikom SGR, zgodnie z art. 7 ust. 3, przed uzyskaniem przez nich dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej;

d) w razie potrzeby zaleca wyjaśnienie każdego zaistniałego lub domniemanego przypadku narażenia na szwank bezpieczeństwa informacji niejawnych znajdujących się w posiadaniu Rady lub wytworzonych przez Radę lub utraty takich informacji oraz zwraca się do właściwych organów bezpieczeństwa o pomoc w takim postępowaniu wyjaśniającym;

e) przeprowadza okresowe inspekcje zabezpieczeń służących ochronie informacji niejawnych w obiektach SGR;

f) przeprowadza okresowe inspekcje zabezpieczeń służących ochronie EUCI w agencjach i organach UE utworzonych na mocy tytułu V rozdział 2 TUE, w Europolu i Eurojuście, jak również podczas operacji zarządzania kryzysowego prowadzonych na mocy tytułu V rozdział 2 TUE oraz zabezpieczeń stosowanych przez specjalnych przedstawicieli UE (SPUE) i członków ich zespołów;

g) przeprowadza, wspólnie i w porozumieniu z zainteresowanymi KWB, okresowe inspekcje zabezpieczeń służących ochronie EUCI w jednostkach organizacyjnych i obiektach w państwach członkowskich;

h) koordynuje środki bezpieczeństwa z właściwymi organami państw członkowskich odpowiedzialnymi za ochronę informacji niejawnych oraz, w stosownych przypadkach, z państwami trzecimi lub organizacjami międzynarodowymi, w tym w zakresie charakteru zagrożeń dla bezpieczeństwa EUCI oraz środków ochrony przed tymi zagrożeniami;

i) zawiera porozumienia administracyjne, o których mowa w art. 12 ust. 2 lit. b); oraz

j) przeprowadza wstępne i okresowe wizyty oceniające w państwach trzecich lub w organizacjach międzynarodowych w celu sprawdzenia skuteczności środków wprowadzonych, by chronić EUCI przekazane im jednostronnie lub w ramach wymiany.

Biuro ds. Bezpieczeństwa SGR pozostaje do dyspozycji Sekretarza Generalnego i pomaga mu w wypełnianiu wyżej opisanych obowiązków.

3. W celu wprowadzenia w życie art. 14 ust. 3 państwa członkowskie powinny:

a) wyznaczyć KWB odpowiedzialną za zabezpieczenia służące ochronie EUCI, tak aby:

(i) EUCI znajdujące się w posiadaniu jakiegokolwiek podmiotu krajowego: departamentu, organu lub agencji, bez względu na to, czy jest to podmiot publiczny czy prywatny i czy znajduje się w kraju czy za granicą, były chronione zgodnie z niniejszą decyzją;

(ii) zabezpieczenia służące ochronie EUCI były poddawane okresowym inspekcjom;

(iii) wszystkie osoby, które są zatrudnione w administracji krajowej lub przez wykonawcę i które mogą uzyskać dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, były odpowiednio sprawdzane lub by przyznano tym osobom ze względu na pełnione przez nie funkcje inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(iv) programy bezpieczeństwa były w razie konieczności opracowane, aby zminimalizować ryzyko narażenia bezpieczeństwa EUCI na szwank lub ich utraty;

(v) kwestie bezpieczeństwa związane z ochroną EUCI były koordynowane z innymi właściwymi organami krajowymi, w tym z organami, o których mowa w niniejszej decyzji; oraz

(vi) rozpatrywane były odpowiednie wnioski o wydanie poświadczenia bezpieczeństwa składane przez agencje i organy UE utworzone na mocy tytułu V rozdział 2 TUE, Europol i Eurojust, jak również składane w ramach operacji zarządzania kryzysowego prowadzonych na mocy tytułu V rozdział 2 TUE oraz składane przez SPUE i ich zespoły.

KWB są wymienione w dodatku C;

b) zapewnić, by ich właściwe organy dostarczały informacje i doradzały rządowi, a za jego pośrednictwem – Radzie co do charakteru zagrożeń dla bezpieczeństwa EUCI i środków ochrony przed tymi zagrożeniami.

Artykuł 16

Komitet ds. Bezpieczeństwa

1. Niniejszym ustanawia się Komitet ds. Bezpieczeństwa. Komitet analizuje i ocenia wszelkie kwestie bezpieczeństwa, które wchodzą w zakres stosowania niniejszej decyzji, oraz przedstawia Radzie odpowiednie zalecenia.

2. Komitet ds. Bezpieczeństwa składa się z przedstawicieli KWB państw członkowskich, a w jego obradach uczestniczy przedstawiciel Komisji i Europejskiej Służby Działań Zewnętrznych. Przewodniczy mu Sekretarz Generalny lub wyznaczona przez niego osoba. Komitet ten zbiera się na polecenie Rady lub na wniosek Sekretarza Generalnego lub KWB.

Do uczestnictwa w obradach komitetu mogą zostać zaproszeni przedstawiciele agencji i organów UE utworzonych na mocy tytułu V rozdział 2 TUE, jak również Europolu i Eurojustu, jeżeli omawiane są kwestie, które ich dotyczą.

3. Komitet ds. Bezpieczeństwa organizuje swoją działalność w taki sposób, aby móc przedstawiać zalecenia w konkretnych dziedzinach dotyczących bezpieczeństwa. Powołuje on podgrupę ekspercką zajmującą się kwestiami zabezpieczania informacji oraz inne podgrupy eksperckie, zależnie od konieczności. Wyznacza on zakres zadań takich podgrup eksperckich i otrzymuje od nich sprawozdania z działalności, w tym – w zależności od sytuacji – zalecenia dla Rady.

Artykuł 17

Zastąpienie poprzedniej decyzji

1. Niniejsza decyzja uchyla i zastępuje decyzję Rady 2001/264/WE z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa ([1]).

2. Wszystkie EUCI opatrzone klauzulą tajności zgodnie z decyzją Rady 2001/264/WE podlegają dalszej ochronie zgodnie z właściwymi przepisami niniejszej decyzji.

Artykuł 18

Wejście w życie

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 31 marca 2011 r.

W imieniu Rady
VÖLNER P.
Przewodniczący

([1]) Dz.U. L 101 z 11.4.2001, s. 1.

ZAŁĄCZNIKI

ZAŁĄCZNIK I

Bezpieczeństwo osobowe

ZAŁĄCZNIK II

Bezpieczeństwo fizyczne

ZAŁĄCZNIK III

Zarządzanie informacjami niejawnymi

ZAŁĄCZNIK IV

Ochrona EUCI przetwarzanych w CIS

ZAŁĄCZNIK V

Bezpieczeństwo przemysłowe

ZAŁĄCZNIK VI

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

ZAŁĄCZNIK I

BEZPIECZEŃSTWO OSOBOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 7. W niniejszym załączniku określa się w szczególności kryteria wykorzystywane do oceny, czy daną osobę ze względu na jej lojalność, wiarygodność i rzetelność można uprawnić do dostępu do EUCI, a także procedury sprawdzające i administracyjne, które należy stosować w tym celu.

2. W całym niniejszym załączniku, z wyjątkiem miejsc, w których rozróżnienie to jest istotne, termin „poświadczenie bezpieczeństwa osobowego" odnosi się do krajowego poświadczenia bezpieczeństwa osobowego (krajowego PBO) lub do poświadczenia bezpieczeństwa osobowego UE (PBO UE) zdefiniowanych w dodatku A.

II. PRZYZNAWANIE UPRAWNIEŃ DO DOSTĘPU DO EUCI

3. Daną osobę można uprawnić do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wyłącznie po tym, jak:

   a) stwierdzono, że spełnia ona zasadę ograniczonego dostępu;

   b) wydano jej PBO do odpowiedniego poziomu lub ze względu na pełnione przez nią funkcje przyznano jej inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

   c) została ona poinformowana o zasadach i procedurach bezpieczeństwa służących ochronie EUCI i potwierdziła, że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji.

4. Każde państwo członkowskie i SGR określają, które stanowiska w ich strukturach wymagają dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, i w związku z tym wymagają uzyskania PBO do odpowiedniego poziomu.

III. WYMOGI DOTYCZĄCE WYDAWANIA POŚWIADCZENIA BEZPIECZEŃSTWA OSOBOWEGO

5. Po otrzymaniu odpowiedniego wniosku KWB lub inne właściwe organy krajowe są odpowiedzialne za zapewnienie, by przeprowadzono postępowanie sprawdzające w odniesieniu do obywateli ich kraju, którym niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej. Normy postępowania sprawdzającego są zgodne z krajowymi przepisami ustawowymi i wykonawczymi.

6. Jeżeli miejsce pobytu danej osoby znajduje się na terytorium innego państwa członkowskiego lub państwa trzeciego, właściwe organy krajowe zwracają się o pomoc do właściwego organu państwa pobytu zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Państwa członkowskie wzajemnie się wspierają w prowadzeniu postępowań sprawdzających zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

7. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość, KWB lub inne właściwe organy krajowe mogą przeprowadzać postępowania sprawdzające w odniesieniu do osób niebędących obywatelami ich kraju, którym niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej. Normy postępowania sprawdzającego są zgodne z krajowymi przepisami ustawowymi i wykonawczymi.

Kryteria postępowania sprawdzającego

8. W celu wydania danej osobie PBO upoważniającego ją do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej sprawdza się jej lojalność, wiarygodność i rzetelność, przeprowadzając postępowanie sprawdzające. Na podstawie wyników takiego postępowania właściwy organ krajowy dokonuje ogólnej oceny. Pojedyncza niekorzystna informacja uzyskana w wyniku postępowania sprawdzającego nie musi skutkować odmową wydania PBO. Główne kryteria stosowane w tym celu powinny obejmować – w zakresie, jaki umożliwiają to krajowe przepisy ustawowe i wykonawcze – ustalenie, czy osoba ta:

   a) popełniła lub usiłowała popełnić akt szpiegostwa, terroryzmu, sabotażu, zdrady lub buntu, współdziałała z inną osobą w celu popełnienia takiego aktu, pomagała innej osobie w jego popełnieniu lub nakłaniała inne osoby do popełnienia takiego aktu;

   b) współdziała lub współdziałała ze szpiegami, terrorystami, sabotażystami lub osobami, co do których istnieje uzasadnione podejrzenie, że nimi są, lub z przedstawicielami organizacji lub obcych państw, w tym obcych służb wywiadowczych, które mogą stanowić zagrożenie dla bezpieczeństwa UE lub państw członkowskich, chyba że udzielono zezwolenia na takie współdziałanie w ramach obowiązków służbowych;

c) jest lub była członkiem organizacji, która za pomocą aktów przemocy, działalności wywrotowej lub innych nielegalnych środków dąży m.in. do obalenia rządu państwa członkowskiego, zmiany porządku konstytucyjnego państwa członkowskiego lub zmiany formy lub polityki jego rządu;

d) jest lub była stronnikiem jakiejkolwiek organizacji opisanej w lit. c) lub blisko współdziała lub blisko współdziałała z członkami takich organizacji;

e) świadomie zataiła, fałszywie przedstawiła lub sfałszowała istotne informacje, szczególnie informacje związane z bezpieczeństwem, lub świadomie skłamała przy wypełnianiu ankiety bezpieczeństwa osobowego lub podczas rozmowy przeprowadzanej w ramach postępowania sprawdzającego;

f) została skazana za popełnienie przestępstwa lub przestępstw;

g) kiedykolwiek była uzależniona od alkoholu, zażywała nielegalne środki odurzające lub nadużywała legalnych środków odurzających;

h) zachowuje się lub zachowywała w sposób mogący stwarzać ryzyko podatności na szantaż lub presję;

i) w czynach lub słowach wykazała się nieuczciwością, nielojalnością, brakiem rzetelności lub wiarygodności;

j) poważnie lub wielokrotnie naruszyła przepisy dotyczące bezpieczeństwa lub usiłowała dokonać albo dokonała czynności, do których nie była uprawniona, w odniesieniu do systemów teleinformatycznych;

k) może podlegać presji (np. poprzez posiadanie jednego lub więcej obywatelstw państw niebędących członkiem UE lub presji krewnych lub bliskich współpracowników, którzy mogą być podatni na wpływy obcych służb wywiadowczych, grup terrorystycznych lub innych wywrotowych organizacji lub osób mogących zagrażać interesom bezpieczeństwa UE lub państw członkowskich).

9. W odpowiednich przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas przeprowadzania postępowania sprawdzającego za istotną można uznać także sytuację finansową i zdrowotną danej osoby.

10. W odpowiednich przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas przeprowadzania postępowania sprawdzającego za istotne można uznać także charakter, zachowanie i sytuację współmałżonka danej osoby, jej partnera życiowego lub członka bliskiej rodziny.

Wymogi dotyczące postępowania sprawdzającego na potrzeby dostępu do EUCI

Wydanie pierwszego PBO

11. Pierwsze PBO upoważniające do dostępu do informacji niejawnych o klauzulach tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET wydawane jest po przeprowadzeniu postępowania sprawdzającego obejmującego co najmniej okres ostatnich pięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy; postępowanie obejmuje:

a) wypełnienie krajowej ankiety bezpieczeństwa osobowego do odpowiedniego poziomu EUCI, do których dostęp może być niezbędny danej osobie; wypełniona ankieta przekazywana jest właściwemu organowi bezpieczeństwa;

b) sprawdzenie tożsamości/obywatelstwa/narodowości – potwierdza się datę i miejsce urodzenia danej osoby i sprawdza się jej tożsamość. Ustala się przeszłe i obecne obywatelstwo lub narodowość danej osoby; obejmuje to ocenę podatności na presję wywieraną przez osoby z zagranicy, na przykład w związku z poprzednim miejscem pobytu lub przeszłymi powiązaniami; oraz

c) sprawdzenie rejestrów krajowych i lokalnych – sprawdzane są krajowe rejestry bezpieczeństwa i centralne rejestry karne, o ile te ostatnie istnieją, lub inne porównywalne rejestry rządowe i policyjne. Sprawdza się rejestry organów ścigania sprawujących jurysdykcję w miejscach, w których dana osoba miała miejsce pobytu lub była zatrudniona.

12. Pierwsze PBO upoważniające do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET wydawane jest po przeprowadzeniu postępowania sprawdzającego obejmującego co najmniej okres ostatnich dziesięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy. Jeżeli zgodnie z lit. e) przeprowadzane są rozmowy, postępowanie sprawdzające obejmuje co najmniej okres ostatnich siedmiu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który okres jest krótszy. Poza kryteriami określonymi w pkt 8 przed wydaniem PBO upoważniającego do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET należy wyjaśnić – w zakresie, w jakim umożliwiają to krajowe przepisy ustawowe i wykonawcze – elementy wymienione poniżej; elementy te można również wyjaśnić przed wydaniem PBO upoważniającego do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, jeżeli wymagają tego krajowe przepisy ustawowe i wykonawcze:

a) status finansowy – poszukuje się informacji dotyczących sytuacji finansowej danej osoby, aby ocenić stopień jej podatności na presję osób z kraju lub z zagranicy z powodu poważnych trudności finansowych lub aby ujawnić wszelkie przychody z nieznanych źródeł;

b) wykształcenie – poszukuje się informacji służących weryfikacji wykształcenia danej osoby w szkołach, szkołach wyższych lub innych placówkach edukacyjnych, do których uczęszczała ona od ukończenia 18. roku życia lub w okresie, który organ prowadzący postępowanie sprawdzające uzna za odpowiedni;

c) zatrudnienie – poszukuje się informacji dotyczących obecnego i poprzedniego zatrudnienia, przy wykorzystaniu takich źródeł jak historia zatrudnienia, sprawozdania dotyczące wyników lub wydajności pracy oraz opinie pracodawców lub przełożonych;

d) służba wojskowa – w stosownych przypadkach weryfikowany jest stosunek danej osoby do służby wojskowej oraz powód zwolnienia ze służby; oraz

e) rozmowy – pod warunkiem że przepisy krajowe przewidują i dopuszczają taką możliwość, przeprowadza się z daną osobą rozmowę lub rozmowy. Rozmowy przeprowadza się również z innymi osobami, które są w stanie przedstawić obiektywną ocenę dotyczącą pochodzenia, działalności, lojalności, wiarygodności i rzetelności osoby sprawdzanej. W przypadku gdy krajowa praktyka przewiduje przedstawianie referencji przez osobę sprawdzaną, przeprowadza się rozmowę z osobami, które dostarczyły tych referencji, chyba że istnieją uzasadnione powody, żeby tego nie czynić.

13. Jeżeli jest to konieczne i zgodne z krajowymi przepisami ustawowymi i wykonawczymi, można przeprowadzić dodatkowe wyjaśnienia w celu rozwinięcia wszelkich dostępnych istotnych informacji dotyczących danej osoby oraz w celu potwierdzenia lub wykazania fałszywości informacji działających na niekorzyść osoby sprawdzanej.

Przedłużanie ważności PBO

14. Po wydaniu pierwszego PBO oraz pod warunkiem że w zatrudnieniu danej osoby w administracji krajowej lub w SGR nie wystąpiły przerwy, a dostęp do EUCI jest jej stale potrzebny, przedłużenie ważności PBO tej osoby rozpatrywane jest w odstępach czasu nieprzekraczających pięciu lat w przypadku poświadczenia do klauzuli tajności TRÈS SECRET UE/EU TOP SECRET oraz dziesięciu lat w przypadku poświadczeń do klauzul tajności SECRET UE/EU SECRET i CONFIDENTIEL UE/EU CONFIDENTIAL, licząc od daty powiadomienia o wyniku ostatniego postępowania sprawdzającego, na podstawie którego zostały wydane te poświadczenia. Wszelkie postępowania sprawdzające dotyczące przedłużenia ważności PBO obejmują okres od poprzedniego postępowania.

15. W celu przedłużenia ważności PBO należy wyjaśnić elementy przedstawione w pkt 11 i 12.

16. Wnioski o przedłużenie ważności składane są z odpowiednim wyprzedzeniem, z uwzględnieniem czasu wymaganego do przeprowadzenia postępowań sprawdzających. Jeżeli jednak odpowiednia KWB lub inny właściwy organ krajowy otrzymały odpowiedni wniosek o przedłużenie ważności oraz właściwą ankietę bezpieczeństwa osobowego, zanim PBO utraciło ważność, a niezbędne postępowanie sprawdzające nie zostało jeszcze zakończone, właściwy organ krajowy może przedłużyć ważność obowiązującego PBO o okres nieprzekraczający 12 miesięcy, jeżeli dopuszczają to krajowe przepisy ustawowe i wykonawcze. Jeżeli na koniec tego 12-miesięcznego okresu nadal nie zakończono postępowania sprawdzającego, danej osobie przyznaje się obowiązki, które nie wymagają posiadania PBO.

Procedury związane z wydaniem PBO w SGR

17. W przypadku urzędników i innych pracowników SGR organ bezpieczeństwa SGR przekazuje wypełnioną ankietę bezpieczeństwa osobowego KWB państwa członkowskiego, którego obywatelem jest dana osoba, z wnioskiem o przeprowadzenie postępowania sprawdzającego do poziomu EUCI, do którego dostęp będzie tej osobie niezbędny.

18. Jeżeli SGR znajdzie się w posiadaniu informacji dotyczącej osoby, która złożyła wniosek o PBO UE, istotnej w odniesieniu do postępowania sprawdzającego, powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.

19. Po zakończeniu postępowania sprawdzającego odpowiednia KWB powiadamia organ bezpieczeństwa SGR, w formacie korespondencji określonym przez Komitet ds. Bezpieczeństwa, o wyniku takiego postępowania.

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 powołujący SGR może wydać tej osobie PBO UE oraz upoważnić ją do dostępu do EUCI do odpowiedniego poziomu i do określonej daty.

b) Jeżeli w wyniku postępowania sprawdzające nie uzyskuje się takiej pewności, organ powołujący SGR powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ powołujący może zwrócić się do właściwej KWB o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się PBO UE.

20. 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 powołującego SGR podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym urzędników Unii Europejskiej i Warunkami zatrudnienia innych pracowników Unii Europejskiej, określonymi w rozporządzeniu (EWG, Euratom, EWWiS) nr 259/68 [1] (zwanymi dalej „regulaminem pracowniczym i warunkami zatrudnienia").

21. Pewność, na podstawie której wydaje się PBO UE, o ile nadal istnieje, odnosi się do każdego zadania powierzonego danej osobie w SGR lub Komisji.

22. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu powołującego SGR o wyniku postępowania sprawdzającego lub jeżeli w pełnieniu obowiązków przez daną osobę występuje 12-miesięczna przerwa, w czasie której osoba ta nie jest zatrudniona w SGR ani na żadnym stanowisku w administracji krajowej państwa członkowskiego, wynik postępowania sprawdzającego jest przekazywany odpowiedniej KWB w celu potwierdzenia, czy nadal pozostaje ważny i właściwy.

23. Jeżeli SGR znajdzie się w posiadaniu informacji o ryzyku naruszenia zasad bezpieczeństwa przez osobę, która posiada ważne PBO UE, powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi. Jeżeli KWB powiadomi SGR o utracie pewności uzyskanej zgodnie z pkt 19 lit. a) w odniesieniu do osoby posiadającej ważne PBO UE, organ powołujący SGR 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, PBO UE 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.

24. O każdej decyzji w sprawie cofnięcia PBO UE przyznanego urzędnikowi lub innemu pracownikowi SGR i, w odpowiednich przypadkach, o przyczynach tego cofnięcia powiadamia się daną osobę, a ona może zwrócić się do organu powołującego z prośbą o wysłuchanie. Informacje przedstawione przez KWB podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu powołującego SGR podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym i warunkami zatrudnienia.

25. Eksperci krajowi oddelegowani do SGR na stanowisko wymagające PBO UE przedstawiają organowi bezpieczeństwa SGR – przed rozpoczęciem wykonywania swoich zadań – ważne krajowe PBO uprawniające do dostępu do EUCI.

Wykazy PBO

26. Wykazy krajowych PBO i PBO UE wydanych w celu umożliwienia dostępu do EUCI są przechowywane, odpowiednio, przez każde państwo członkowskie i przez SGR. Wykazy te zawierają co najmniej informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), dacie wydania PBO i okresie jego ważności.

27. Właściwy organ bezpieczeństwa może wydać zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego (ZPBO) zawierające informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okresie ważności odpowiedniego krajowego PBO umożliwiającego dostęp do EUCI lub PBO UE oraz dacie ważności samego zaświadczenia.

Zwolnienia z wymogu posiadania PBO

28. Dostęp do EUCI osób odpowiednio upoważnionych ze względu na pełnione przez siebie funkcje w państwach członkowskich określany jest zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; osoby takie są informowane o spoczywających na nich obowiązkach dotyczących bezpieczeństwa polegających na ochronie EUCI.

IV. SZKOLENIA I UPOWSZECHNIANIE WIEDZY W ZAKRESIE BEZPIECZEŃSTWA

29. Wszystkie osoby, którym wydano PBO, oświadczają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank bezpieczeństwa EUCI. Wykaz pisemnych oświadczeń przechowywany jest, odpowiednio, przez państwo członkowskie i przez SGR.

30. Wszystkie osoby, które są upoważnione do dostępu do EUCI lub muszą wykorzystywać te informacje, na początku powiadamiane są o zagrożeniach bezpieczeństwa, a następnie regularnie szkolone w zakresie tych zagrożeń; osoby te muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe.

31. Wszystkie osoby, które przestają wykonywać obowiązki wymagające dostępu do EUCI, powiadamiane są o obowiązku stałej ochrony EUCI; w odpowiednich przypadkach świadomość tego obowiązku potwierdzają one na piśmie.

[1] Dz.U. L 56 z 4.3.1968, s. 1.

V. WYJĄTKOWE OKOLICZNOŚCI

32. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość, poświadczenie bezpieczeństwa osobowego wydane przez właściwy organ krajowy państwa członkowskiego i uprawniające do dostępu do krajowych informacji niejawnych może, podczas oczekiwania na wydanie krajowego PBO uprawniającego do dostępu do EUCI, tymczasowo uprawniać urzędników krajowych do dostępu do EUCI do poziomu odpowiadającego poziomowi określonemu w tabeli odpowiedników klauzul tajności, którą zamieszczono w dodatku B, o ile takiego tymczasowego dostępu wymaga interes UE. Jeżeli krajowe przepisy ustawowe i wykonawcze nie zezwalają na taki tymczasowy dostęp do EUCI, KWB informują o tym Komitet ds. Bezpieczeństwa.

33. W nagłych przypadkach, jeżeli jest to należycie uzasadnione interesami jednostki organizacyjnej, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ powołujący SGR może, po konsultacji z KWB państwa członkowskiego, którego obywatelem jest dana osoba, oraz z zastrzeżeniem, że wynik wstępnego sprawdzenia nie wykazał niekorzystnych informacji, wydać urzędnikom i innym pracownikom SGR tymczasowe upoważnienie do dostępu do EUCI, by mogli wykonać określone zadania. Takie tymczasowe upoważnienia zachowują ważność przez okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET. 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 SGR.

34. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie o jeden wyższym niż aktualnie posiadany przez nią, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem, pod warunkiem że:

    a) bezwzględna potrzeba dostępu do EUCI o wyższej klauzuli tajności jest uzasadniona na piśmie przez przełożonego tej osoby;

    b) dostęp jest ograniczony do konkretnych EUCI, które są potrzebne do pracy na tym stanowisku;

    c) osoba ta posiada ważne krajowe PBO lub PBO UE;

    d) podjęto czynności w celu uzyskania upoważnienia do dostępu do informacji na poziomie wymaganym na tym stanowisku;

    e) właściwy organ dokonał sprawdzenia, które potwierdziło, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa;

    f) objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ; oraz

    g) dokumentacja dotycząca przyznania dostępu w drodze wyjątku, wraz z opisem informacji, do których zatwierdzono dostęp, przechowywana jest w odpowiedzialnej kancelarii tajnej lub podległej kancelarii tajnej.

35. Powyższa procedura jest stosowana, by przyznać danej osobie jednorazowy dostęp do EUCI o klauzuli tajności o jeden poziom wyższej niż klauzula, do której ma ona dostęp po dokonaniu odpowiedniego sprawdzenia. Z procedury tej nie korzysta się w sposób wielokrotny.

36. W szczególnie wyjątkowych okolicznościach, takich jak misje prowadzone we wrogim środowisku lub w okresie rosnącego napięcia międzynarodowego, i gdy wymagają tego środki nadzwyczajne, w szczególności w celu ratowania życia ludzkiego, państwa członkowskie i Sekretarz Generalny mogą udzielić, w miarę możliwości na piśmie, dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET osobom, które nie posiadają wymaganego PBO, pod warunkiem że takie zezwolenie jest absolutnie niezbędne i nie ma żadnych uzasadnionych wątpliwości co do lojalności, wiarygodności i rzetelności danej osoby. Zachowuje się dokumentację takiego zezwolenia zawierającą opis informacji, do których dostęp zatwierdzono.

37. Taki dostęp w sytuacjach nadzwyczajnych do informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET przysługuje tylko obywatelom UE, których upoważniono do dostępu do informacji niejawnych o klauzuli krajowej odpowiadającej klauzuli tajności TRÈS SECRET UE/EU TOP SECRET albo do informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET.

38. Komitet ds. Bezpieczeństwa informowany jest o przypadkach skorzystania z procedury przedstawionej w pkt 36 i 37.

39. Jeżeli krajowe przepisy ustawowe i wykonawcze państwa członkowskiego przewidują bardziej rygorystyczne zasady dotyczące tymczasowych upoważnień, tymczasowego pełnienia obowiązków, jednorazowego dostępu do informacji niejawnych lub dostępu do takich informacji w sytuacjach nadzwyczajnych, procedury przewidziane w niniejszej sekcji stosowane są wyłącznie w ramach ograniczeń ustalonych w odpowiednich przepisach ustawowych i wykonawczych.

40. Komitet ds. Bezpieczeństwa otrzymuje roczne sprawozdanie na temat korzystania z procedur określonych w niniejszej sekcji.

VI. UDZIAŁ W POSIEDZENIACH NA FORUM RADY

41. Z zastrzeżeniem pkt 28, osoby wyznaczone do udziału w posiedzeniach Rady lub organów przygotowawczych Rady, podczas których omawiane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, mogą brać w nich udział tylko po potwierdzeniu statusu ich PBO. W przypadku delegatów ich ZPBO lub inny dowód posiadania przez nich PBO przesyłany jest przez odpowiednie organy do Biura ds. Bezpieczeństwa SGR lub, w sytuacjach wyjątkowych, przedstawiany jest przez samego delegata. W stosownych przypadkach można zastosować skonsolidowany wykaz nazwisk, przedstawiając odpowiednie dowody posiadania PBO.

42. Jeżeli z powodów bezpieczeństwa osobie, której obowiązki wymagają udziału w posiedzeniach Rady lub organów przygotowawczych Rady, cofnięte zostaje krajowe PBO uprawniające do dostępu do EUCI, właściwy organ informuje o tym SGR.

VII. POTENCJALNY DOSTĘP DO EUCI

43. Osoby, które mają zostać zatrudnione w warunkach stwarzających potencjalny dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, zostają odpowiednio sprawdzone lub przez cały czas towarzyszy im eskorta.

44. Kurierzy, strażnicy i eskorta są sprawdzani do odpowiedniego poziomu lub w inny sposób odpowiednio sprawdzani zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, informowani o procedurach bezpieczeństwa w zakresie ochrony EUCI oraz instruowani o obowiązku ochrony informacji, które im powierzono.

ZAŁĄCZNIK II

BEZPIECZEŃSTWO FIZYCZNE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 8. Określa on minimalne wymogi w zakresie fizycznej ochrony obiektów, budynków, biur, pomieszczeń i innych stref, w których EUCI są wykorzystywane i przechowywane, w tym stref, w których znajdują się CIS.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie nieuprawnionemu dostępowi do EUCI przez:

   a) zapewnienie właściwego wykorzystywania i przechowywania EUCI;

   b) umożliwienie podziału pracowników pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu i, w odpowiednich przypadkach, posiadanym przez nich poświadczeniem bezpieczeństwa;

   c) powstrzymywanie nieuprawnionych działań, ich udaremnianie i wykrywanie; oraz

   d) uniemożliwienie lub opóźnienie wtargnięcia osób nieupoważnionych w sposób niezauważony lub z użyciem siły.

II. WYMOGI I ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

3. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy. SGR i państwa członkowskie stosują w swoich obiektach proces zarządzania ryzykiem służący ochronie EUCI, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. Proces zarządzania ryzykiem uwzględnia wszystkie 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 ochrony;

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

   d) szacowane zagrożenie ze strony służb wywiadowczych, których celem jest UE lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.

4. Stosując koncepcję ochrony w głąb, właściwy organ bezpieczeństwa określa właściwą kombinację środków bezpieczeństwa fizycznego, które należy zastosować. Mogą one obejmować jeden z poniższych środków lub większą ich liczbę:

   a) ogrodzenie: fizyczne ogrodzenie, które chroni granice strefy wymagającej ochrony;

   b) systemy sygnalizacji włamania i napadu (SSWiN): SSWiN można stosować w celu podwyższenia poziomu bezpieczeństwa, który daje ogrodzenie, a w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników ochrony;

   c) kontrola dostępu: kontrola dostępu może obejmować teren, budynek lub budynki znajdujące się na danym terenie lub też strefy lub pomieszczenia wewnątrz budynku. Kontrolę można prowadzić za pomocą środków elektronicznych, środków elektromechanicznych, za pośrednictwem pracowników ochrony lub pracowników recepcji lub za pomocą wszelkich innych środków fizycznych;

   d) pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności odpowiednio sprawdzeni pracownicy ochrony mogą być zatrudniani, między innymi w celu powstrzymania osób planujących niezauważone wejście na dany teren;

   e) telewizja przemysłowa (CCTV): CCTV może być stosowana przez pracowników ochrony w celu sprawdzania incydentów i sygnałów alarmowych pochodzących z SSWiN na rozległych terenach lub na ogrodzeniach;

   f) oświetlenie ochronne: oświetlenie ochronne może być stosowane w celu powstrzymania potencjalnych osób nieupoważnionych, a ponadto w celu zapewnienia oświetlenia koniecznego do prowadzenia skutecznego nadzoru bezpośrednio przez pracowników ochrony lub pośrednio za pomocą systemu CCTV; oraz

   g) wszelkie inne stosowne środki fizyczne służące powstrzymywaniu lub wykrywaniu przypadków nieuprawnionego dostępu lub zapobieganiu utracie EUCI lub narażeniu na szwank ich bezpieczeństwa.

5. Właściwy organ może być uprawniony do przeprowadzania przeszukania osób wchodzących i wychodzących, co ma stanowić środek odstraszający przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z obiektów lub budynków.

6. Jeżeli istnieje ryzyko podglądu EUCI, także przypadkowego, podejmuje się stosowne środki w celu zlikwidowania takiego ryzyka.

7. W przypadku nowych obiektów wymogi dotyczące bezpieczeństwa fizycznego i specyfikacje dotyczące ich stosowania określane są w ramach planowania i projektowania tych obiektów. W przypadku obiektów już istniejących wymogi dotyczące bezpieczeństwa fizycznego stosowane są w największym możliwym zakresie.

III. SPRZĘT SŁUŻĄCY DO FIZYCZNEJ OCHRONY EUCI

8. Przy zakupie sprzętu służącego do fizycznej ochrony EUCI (takiego jak zabezpieczone szafy, niszczarki, zamki do drzwi, elektroniczne systemy kontroli dostępu, SSWiN, systemy alarmowe) właściwy organ bezpieczeństwa zapewnia, by sprzęt ten spełniał zatwierdzone normy techniczne i minimalne wymogi.

9. Specyfikacje techniczne sprzętu, który ma być wykorzystywany do fizycznej ochrony EUCI, określane są w wytycznych dotyczących bezpieczeństwa, które zatwierdza Komitet ds. Bezpieczeństwa.

10. Systemy bezpieczeństwa są poddawane regularnym inspekcjom, a sprzęt – regularnej konserwacji. Podczas konserwacji uwzględnia się wyniki inspekcji, aby zapewnić dalsze optymalne działanie sprzętu.

11. Podczas każdej inspekcji przeprowadza się ocenę skuteczności poszczególnych środków bezpieczeństwa oraz całego systemu bezpieczeństwa.

IV. STREFY CHRONIONE FIZYCZNIE

12. Ustanawia się dwa rodzaje stref chronionych fizycznie lub ich krajowych odpowiedników, służących fizycznej ochronie EUCI:

    a) strefy administracyjne; oraz

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

    W niniejszej decyzji wszystkie odniesienia do stref administracyjnych i stref bezpieczeństwa, w tym stref technicznie zabezpieczonych, należy rozumieć jako odnoszące się także do ich krajowych odpowiedników.

13. Właściwy organ bezpieczeństwa stwierdza, czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną, strefę bezpieczeństwa lub strefę technicznie zabezpieczoną.

14. 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 właściwy organ; oraz

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

15. 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 i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z zasadą ograniczonego dostępu;

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

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

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

    b) wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie do wejścia do tej strefy, przez cały czas towarzyszyć im musi eskorta i muszą być odpowiednio sprawdzone, chyba że podjęte zostały kroki służące zapewnieniu, aby nie był możliwy dostęp do EUCI.

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

    a) strefy takie wyposażone są w SSWiN, są zamknięte na klucz, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa. Wszystkie klucze podlegają kontroli zgodnie z sekcją VI;

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

    c) strefy takie podlegają regularnym inspekcjom fizycznym lub technicznym zgodnie z wymogami właściwego organu bezpieczeństwa. 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 niezatwierdzone linie komunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.

18. Niezależnie od pkt 17 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 o klauzuli tajności SECRET UE/EU SECRET i wyższej, a także jeżeli ocenia się, że istnieje wysokie zagrożenie dla EUCI, urządzenia i sprzęt taki zostają najpierw sprawdzone przez właściwy organ bezpieczeństwa w celu zapewnienia, aby żadne zrozumiałe informacje nie zostały nieumyślnie lub nielegalnie transmitowane przez taki sprzęt poza granicę strefy bezpieczeństwa.

19. 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.

20. 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.

21. Dla każdej strefy bezpieczeństwa opracowywane są procedury bezpiecznej eksploatacji określające:

    a) poziom klauzuli tajności EUCI, które można wykorzystywać i przechowywać w tej strefie;

    b) środki nadzoru i ochrony, które należy stosować;

    c) osoby upoważnione do wejścia do strefy bez eskorty ze względu na zasadę ograniczonego dostępu i posiadane poświadczenie 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.

22. W ramach stref bezpieczeństwa są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i wyposażone w zamek drzwi zatwierdzane są przez właściwy organ bezpieczeństwa i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI o tym samym poziomie klauzuli tajności.

V. FIZYCZNE ŚRODKI OCHRONY NA POTRZEBY WYKORZYSTYWANIA I PRZECHOWYWANIA EUCI

23. Wykorzystywanie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED może się odbywać:

    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 przewozi EUCI zgodnie z załącznikiem III pkt 28–40 i zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI.

24. EUCI o klauzuli 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 bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa.

25. Wykorzystywanie EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET może się odbywać:

    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) przewozi EUCI zgodnie z załącznikiem III pkt 28–40;

        (ii) zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwy organ bezpieczeństwa służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI;

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

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

26. EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są w strefie bezpieczeństwa w zabezpieczonej szafie lub wzmocnionym pomieszczeniu.

27. Wykorzystywanie EUCI o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET odbywa się w strefie bezpieczeństwa.

28. EUCI o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET przechowywane są w strefie bezpieczeństwa, przy spełnieniu jednego z następujących warunków:

    a) są one przechowywane w zabezpieczonej szafie, zgodnie z pkt 8, wyposażonym w co najmniej jedno z następujących zabezpieczeń dodatkowych:

        (i) stała ochrona lub kontrola przez odpowiednio sprawdzonych pracowników ochrony lub pracowników pełniących dyżur;

        (ii) zatwierdzony SSWiN obsługiwany przez pracowników ochrony odpowiedzialnych za bezpieczeństwo;

    lub

    b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN oraz obsługiwanym przez pracowników ochrony odpowiedzialnych za bezpieczeństwo.

29. Przepisy regulujące przewożenie EUCI poza strefy chronione fizycznie znajdują się w załączniku III.

VI. KONTROLA KLUCZY I KODÓW WYKORZYSTYWANYCH DO OCHRONY EUCI

30. Właściwy organ bezpieczeństwa określa procedury zarządzania kluczami i kodami do biur, pomieszczeń, wzmocnionych pomieszczeń i zabezpieczonych szaf. Procedury te chronią przed nieuprawnionym dostępem do informacji.

31. Kody są zapamiętywane przez jak najmniejszą liczbę osób, którym ich znajomość jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, są zmieniane:

    a) przy każdej zmianie pracowników znających kod;

    b) w każdym przypadku, gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji;

    c) gdy zamek poddano konserwacji lub naprawie; oraz

    d) co najmniej co 12 miesięcy.

ZAŁĄCZNIK III

ZARZĄDZANIE INFORMACJAMI NIEJAWNYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 9. Określa on środki administracyjne służące kontroli EUCI na wszystkich etapach ich cyklu życia, co ma pomóc w powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa takich informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków.

II. ZARZĄDZANIE KLAUZULAMI TAJNOŚCI

Klauzule tajności i oznaczenia

2. Informacjom nadaje się klauzulę tajności, jeżeli należy chronić ich poufność.

3. Za określenie poziomu klauzuli tajności, zgodnie z odpowiednimi wytycznymi w zakresie nadawania klauzul, i za początkową dystrybucję informacji odpowiada wytwórca EUCI.

4. Poziom klauzuli tajności EUCI określa się zgodnie z art. 2 ust. 2 i poprzez odniesienie do polityki bezpieczeństwa, która ma być zatwierdzona zgodnie z art. 3 ust. 3.

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

6. Poszczególne części danego dokumentu (np. strony, punkty, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia) mogą wymagać nadania różnych klauzul tajności i zostają odpowiednio oznaczone, także wtedy, gdy są przechowywane w formie elektronicznej.

7. 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.

8. 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 konieczności rozdzielić.

9. Klauzula tajności pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula tajności nadana tym 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

RESTREINT UE/EU RESTRICTED bez załącznika(-ów)

Oznaczenia

10. Oprócz jednej z klauzul tajności określonych w art. 2 ust. 2 EUCI mogą być opatrzone dodatkowymi oznaczeniami, takimi jak:

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 odpowiednich przypadkach data lub konkretne wydarzenie, po których klauzula tajności może zostać obniżona lub zniesiona.

Skrócone oznaczenia klauzul tajności

11. W celu nadania poziomu klauzuli tajności pojedynczym ustępom tekstu można stosować standardowe skrócone oznaczenia klauzul tajności. Skróty nie zastępują pełnych nazw klauzul tajności.

12. W celu wskazania poziomu klauzuli tajności sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach niejawnych UE można stosować następujące standardowe skróty:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Wytwarzanie EUCI

13. Przy wytwarzaniu dokumentu niejawnego UE:

a) każdą stronę wyraźnie oznacza się klauzulą tajności;

b) strony numeruje się;

c) na dokumencie umieszcza się numer referencyjny 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 o klauzuli tajności SECRET UE/EU SECRET lub wyższej, które mają zostać rozpowszechnione w kilku kopiach, umieszcza się numer kopii.

14. Jeżeli do EUCI nie można zastosować pkt 13, podejmowane są inne odpowiednie środki zgodnie z wytycznymi dotyczącymi bezpieczeństwa, które należy ustalić na mocy art. 6 ust. 2.

Obniżanie i znoszenie klauzul tajności EUCI

15. W momencie wytwarzania EUCI wytwórca wskazuje, o ile to możliwe, a w szczególności w odniesieniu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, czy z daną datą lub w następstwie konkretnego wydarzenia klauzula tajności EUCI może zostać obniżona lub zniesiona.

16. SGR przeprowadza regularne przeglądy EUCI znajdujących się w jego posiadaniu, by stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. SGR tworzy system służący do przeglądu klauzul tajności nadanych zarejestrowanym EUCI, których jest wytwórcą, nie rzadziej niż co pięć lat. Taki 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.

III. REJESTRACJA EUCI ZE WZGLĘDÓW BEZPIECZEŃSTWA

17. Dla każdej jednostki organizacyjnej w SGR i w administracji krajowej państw członkowskich, w których wykorzystuje się EUCI, określa się odpowiedzialną kancelarię tajną, która zapewnia, by wykorzystywanie EUCI było zgodne z niniejszą decyzją. Kancelarie tajne uznaje się za strefy bezpieczeństwa określone w załączniku II.

18. Do celów niniejszej decyzji rejestracja ze względów bezpieczeństwa (zwana dalej „rejestracją") oznacza stosowanie procedur rejestrowania etapów cyklu życia tego materiału, w tym jego dystrybucji i zniszczenia.

19. Wszystkie materiały o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej rejestruje się w wyznaczonych kancelariach tajnych w momencie ich wpłynięcia do jednostki organizacyjnej lub wysłania z tej jednostki.

20. Główna kancelaria tajna w SGR prowadzi rejestr wszystkich informacji niejawnych udostępnionych przez Radę i SGR państwom trzecim i organizacjom międzynarodowym i wszystkich informacji niejawnych otrzymanych od tych państw i organizacji.

21. W przypadku CIS procedury rejestracji mogą być stosowane w ramach działań samego CIS.

22. Rada zatwierdza politykę bezpieczeństwa dotyczącą rejestrowania EUCI ze względów bezpieczeństwa.

Kancelarie tajne TRÈS SECRET UE/EU TOP SECRET

23. W państwach członkowskich i w SGR wyznacza się kancelarię tajną będącą głównym organem otrzymującym i przesyłającym informacje niejawne o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET. W razie konieczności można wyznaczyć podległe kancelarie tajne do wykorzystywania takich informacji do celów rejestracji.

24. Takie podległe kancelarie tajne nie mogą przekazywać dokumentów o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET bezpośrednio innym podległym kancelariom tajnym podlegającym tej samej głównej kancelarii tajnej TRÈS SECRET UE/EU TOP SECRET ani na zewnątrz bez wyraźnego pisemnego upoważnienia z jej strony.

IV. KOPIOWANIE I TŁUMACZENIE DOKUMENTÓW NIEJAWNYCH UE

25. Dokumenty o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET nie mogą być kopiowane ani tłumaczone bez wcześniejszej pisemnej zgody ich wytwórcy.

26. Jeżeli wytwórca dokumentów o klauzuli tajności SECRET UE/EU SECRET i niższej nie zgłosił zastrzeżeń co do ich kopiowania lub tłumaczenia, dokumenty takie można kopiować lub tłumaczyć na zlecenie posiadacza.

27. Środki bezpieczeństwa, które stosuje się do oryginału dokumentu, mają zastosowanie do jego kopii i tłumaczeń.

V. PRZEWOŻENIE EUCI

28. Przewożenie EUCI podlega środkom ochrony określonym w pkt 30–40. Gdy EUCI są przewożone z użyciem środków elektronicznych, niezależnie od przepisów art. 9 ust. 4, poniższe środki ochrony mogą być uzupełnione odpowiednimi technicznymi środkami zaradczymi zgodnie z wytycznymi właściwego organu bezpieczeństwa, tak aby zminimalizować ryzyko utraty lub narażenia na szwank bezpieczeństwa informacji.

29. Właściwe organy bezpieczeństwa w SGR i w państwach członkowskich wydają instrukcje dotyczące przewożenia EUCI zgodnie z niniejszą decyzją.

W obrębie budynku lub grupy budynków stanowiącej zamkniętą całość

30. EUCI przewożone w ramach budynku lub grupy budynków stanowiącej zamkniętą całość są zakrywane, aby nie można było zobaczyć ich treści.

31. W ramach budynku lub grupy budynków stanowiącej zamkniętą całość informacje niejawne o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET są przewożone w zabezpieczonej kopercie, na której znajduje się jedynie nazwisko adresata.

Na terytorium UE

32. EUCI przewożone między budynkami lub obiektami na terytorium UE są opakowane w taki sposób, by chronić je przed nieuprawnionym ujawnieniem.

33. Przewóz informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET na terytorium UE odbywa się za pomocą jednego z następujących środków:

a) za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych;

b) osobiście, pod warunkiem że:

(i) EUCI przez cały czas znajdują się w posiadaniu osoby przewożącej je, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku II;

(ii) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych;

(iii) właściwe osoby informuje się o ich obowiązkach w zakresie bezpieczeństwa;

(iv) w odpowiednich przypadkach właściwym osobom wydaje się list kurierski;

c) za pośrednictwem usług pocztowych lub prywatnych służb kurierskich, pod warunkiem że:

(i) są one zatwierdzone przez odpowiednią KWB zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(ii) stosują one odpowiednie środki ochrony zgodnie z minimalnymi wymogami, które mają być ustalone w wytycznych dotyczących bezpieczeństwa na mocy art. 6 ust. 2.

W przypadku przewozu z jednego państwa członkowskiego do drugiego przepisy lit. c) są ograniczone do informacji niejawnych o klauzuli tajności do poziomu CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Materiał oznaczony klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET (np. sprzęt lub urządzenia), który nie może być przewożony środkami, o których mowa w pkt 33, jest transportowany tak jak ładunek przez prywatne firmy przewozowe zgodnie z załącznikiem V.

35. Przewóz informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET między budynkami lub obiektami na terytorium UE odbywa się za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych.

Z terytorium UE na terytorium państwa trzeciego

36. EUCI przewożone z terytorium UE na terytorium państwa trzeciego są opakowane w taki sposób, by chronić je przed nieuprawnionym ujawnieniem.

37. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET z terytorium UE na terytorium państwa trzeciego odbywa się za pomocą jednego z następujących środków:

a) za pośrednictwem kurierów wojskowych lub dyplomatycznych;

b) osobiście, pod warunkiem że:

(i) przesyłka opatrzona jest urzędową pieczęcią lub sposób zapakowania wskazuje na to, że jest to przesyłka urzędowa i nie powinna podlegać kontroli celnej ani kontroli bezpieczeństwa;

(ii) właściwa osoba posiada list kurierski zawierający informacje o przesyłce i upoważniający ją do przewożenia tej przesyłki;

(iii) EUCI przez cały czas znajdują się w posiadaniu osoby przewożącej je, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku II;

(iv) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych;

(v) właściwe osoby informuje się o ich obowiązkach w zakresie bezpieczeństwa.

38. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET udostępnionych przez UE państwu trzeciemu lub organizacji międzynarodowej spełnia odpowiednie przepisy umowy o bezpieczeństwie informacji lub porozumienia administracyjnego zgodnie z art. 12 ust. 2 lit. a) lub b).

39. Informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED mogą być przewożone także za pośrednictwem usług pocztowych lub prywatnych służb kurierskich.

40. Przewóz informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET z terytorium UE na terytorium państwa trzeciego odbywa się za pośrednictwem kurierów wojskowych lub dyplomatycznych.

VI. NISZCZENIE EUCI

41. Dokumenty niejawne UE, które nie są już potrzebne, mogą zostać zniszczone bez uszczerbku dla odpowiednich zasad i przepisów wykonawczych dotyczących archiwizowania.

42. Dokumenty podlegające rejestracji zgodnie z art. 9 ust. 2 są niszczone przez odpowiedzialną kancelarię tajną na polecenie posiadacza lub właściwego organu. Rejestry i inne informacje dotyczące rejestracji są odpowiednio uaktualniane.

43. W odniesieniu do dokumentów niejawnych o klauzuli tajności SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET niszczenie przebiega w obecności świadka, który został odpowiednio sprawdzony co najmniej do poziomu klauzuli tajności niszczonego dokumentu.

44. Osoba dokonująca rejestracji oraz świadek, jeżeli jego obecność jest wymagana, podpisują protokół zniszczenia, który zostaje umieszczony w dokumentacji kancelarii tajnej. Protokoły zniszczenia dokumentów o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET przechowuje się w kancelarii tajnej przez okres co najmniej dziesięciu lat, a dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET – przez okres co najmniej pięciu lat.

45. Dokumenty niejawne, w tym dokumenty o klauzuli tajności RESTREINT UE/EU RESTRICTED, są niszczone przy zastosowaniu metod, które spełniają odpowiednie normy UE lub normy równoważne lub które zostały zatwierdzone przez państwa członkowskie zgodnie z krajowymi normami technicznymi, tak by nie mogły zostać całkowicie lub częściowo odtworzone.

46. Niszczenie komputerowych nośników EUCI odbywa się zgodnie z załącznikiem IV pkt 36.

VII. INSPEKCJE I WIZYTY OCENIAJĄCE

47. Użycie terminu „inspekcja" oznacza poniżej każdą:

a) inspekcję zgodnie z art. 9 ust. 3 oraz art. 15 ust. 2 lit. e), f) i g); lub

b) wizytę oceniającą zgodnie z art. 12 ust. 5,

służącą ocenie skuteczności środków wdrożonych, aby chronić EUCI.

48. Inspekcje przeprowadza się m.in., aby:

a) zapewnić przestrzeganie określonych w niniejszej decyzji wymaganych norm minimalnych w zakresie ochrony EUCI;

b) podkreślić znaczenie bezpieczeństwa i skutecznego zarządzania ryzykiem wewnątrz kontrolowanych podmiotów;

c) zalecić środki zaradcze mające złagodzić konkretne skutki, jakie może powodować utrata poufności, integralności lub dostępności informacji niejawnych; oraz

d) ulepszyć istniejące programy, opracowane przez organy bezpieczeństwa, dotyczące szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa.

49. Przed końcem każdego roku kalendarzowego Rada przyjmuje na następny rok program inspekcji przewidziany w art. 15 ust. 1 lit. c). Konkretne terminy każdej inspekcji są określane w porozumieniu z daną agencją lub organem UE, państwem członkowskim, państwem trzecim lub organizacją międzynarodową.

Prowadzenie inspekcji

50. Inspekcje przeprowadzane są, aby sprawdzić odpowiednie zasady, przepisy i procedury stosowane przez kontrolowany podmiot oraz stwierdzić, czy praktyki w nim stosowane odpowiadają podstawowym zasadom i minimalnym normom określonym w niniejszej decyzji i przepisom dotyczącym wymiany informacji niejawnych z tym podmiotem.

51. Inspekcje są przeprowadzane w dwóch etapach. Przed samą inspekcją w razie potrzeby organizowane jest posiedzenie przygotowawcze z odpowiednim podmiotem. Po spotkaniu przygotowawczym zespół kontrolny ustala, w porozumieniu z wymienionym podmiotem, szczegółowy program inspekcji obejmujący wszystkie obszary bezpieczeństwa. Zespół kontrolny ma dostęp do wszystkich miejsc, w których wykorzystywane są EUCI, w szczególności do kancelarii tajnych i punktów, w których znajdują się CIS.

52. Odpowiedzialność za prowadzenie inspekcji w krajowych administracjach państw członkowskich ponosi wspólny zespół kontrolny SGR i Komisji w pełni współpracujący z urzędnikami kontrolowanego podmiotu.

53. Odpowiedzialność za prowadzenie inspekcji w państwach trzecich i organizacjach międzynarodowych ponosi wspólny zespół kontrolny SGR i Komisji w pełni współpracujący z urzędnikami kontrolowanego państwa trzeciego lub kontrolowanej organizacji międzynarodowej.

54. Inspekcje agencji i organów UE utworzonych na mocy tytułu V rozdział 2 TUE, jak również Europolu i Eurojustu, prowadzone są przez Biuro ds. Bezpieczeństwa SGR przy wsparciu ekspertów KWB państwa, na terytorium którego znajduje się agencja lub organ. W inspekcji może brać udział dyrekcja ds. bezpieczeństwa Komisji Europejskiej (ECSD), jeżeli prowadzi regularną wymianę EUCI z daną agencją lub organem.

55. W przypadku inspekcji w agencjach i organach UE utworzonych na mocy tytułu V rozdział 2 TUE, jak również w Europolu i Eurojuście, oraz w państwach trzecich i organizacjach międzynarodowych eksperci KWB są proszeni o wsparcie i wkład zgodnie ze szczegółowymi ustaleniami uzgodnionymi przez Komitet ds. Bezpieczeństwa.

Raporty z inspekcji

56. Pod koniec inspekcji kontrolowanemu podmiotowi przedstawiane są główne wnioski i zalecenia. Następnie pod nadzorem organu bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) sporządzany jest raport z inspekcji. W przypadku gdy zostały zaproponowane działanie naprawcze i zalecenia, w raporcie zamieszcza się odpowiednio szczegółowe dane uzasadniające dojście do takich wniosków. Raport przekazywany jest właściwemu organowi kontrolowanego podmiotu.

57. W przypadku inspekcji przeprowadzanych w krajowych administracjach państw członkowskich:

a) projekt raportu z inspekcji zostanie przekazany odpowiedniej KWB w celu sprawdzenia, czy jest zgodny z faktami i czy nie zawiera informacji o klauzuli tajności wyższej niż RESTREINT UE/EU RESTRICTED;

b) o ile KWB danego państwa członkowskiego nie wystąpi o wstrzymanie ogólnej dystrybucji, raporty z inspekcji przekazywane są członkom Komitetu ds. Bezpieczeństwa oraz ECSD; raportowi nadaje się klauzulę tajności RESTREINT UE/EU RESTRICTED;

Pod nadzorem organu bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) przygotowywany jest okresowy raport mający na celu uwypuklenie doświadczeń nabytych w wyniku inspekcji przeprowadzonych w państwach członkowskich w danym okresie i przeanalizowanych przez Komitet ds. Bezpieczeństwa.

58. W przypadku wizyt oceniających w państwach trzecich i organizacjach międzynarodowych raport przekazywany jest członkom Komitetu ds. Bezpieczeństwa oraz ECSD. Raportowi nadaje się co najmniej klauzulę tajności RESTREINT UE/EU RESTRICTED. Wszystkie działania naprawcze są weryfikowane podczas kolejnej wizyty, a raport na ich temat przekazywany jest Komitetowi ds. Bezpieczeństwa.

59. W przypadku inspekcji w agencjach i organach UE utworzonych na mocy tytułu V rozdział 2 TUE, jak również w Europolu i Eurojuście, raport z inspekcji przekazywany jest członkom Komitetu ds. Bezpieczeństwa oraz ECSD. Projekt raportu z inspekcji przekazywany jest odpowiedniej agencji lub odpowiedniemu organowi w celu sprawdzenia, czy jest on zgodny z faktami i czy nie zawiera informacji o klauzuli tajności wyższej niż RESTREINT UE/EU RESTRICTED. Wszystkie działania naprawcze są weryfikowane podczas kolejnej wizyty, a raport na ich temat przekazywany jest Komitetowi ds. Bezpieczeństwa.

60. Organ bezpieczeństwa SGR przeprowadza regularne inspekcje jednostek organizacyjnych w SGR w celach określonych w pkt 48.

Lista kontrolna

61. Organ bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) sporządza i uaktualnia listę kontrolną wykorzystywaną podczas inspekcji bezpieczeństwa i zawierającą kwestie, które należy sprawdzić w trakcie inspekcji. Lista kontrolna przekazywana jest Komitetowi ds. Bezpieczeństwa.

62. Informacji służących uzupełnieniu listy kontrolnej udziela, w szczególności podczas inspekcji, personel zajmujący się kontrolą bezpieczeństwa w jednostce, w której przeprowadzana jest inspekcja. Po wypełnieniu listy kontrolnej szczegółowymi odpowiedziami nadaje się jej klauzulę tajności w porozumieniu z kontrolowaną jednostką. Lista ta nie jest częścią raportu z inspekcji.

ZAŁĄCZNIK IV

OCHRONA EUCI PRZETWARZANYCH W CIS

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 10.

2. Następujące cechy i koncepcje zabezpieczania informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach CIS:

Autentyczność:	gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł;
Dostępność:	cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu;
Poufność:	cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom, podmiotom ani do celów nieuprawnionego przetwarzania;
Integralność:	cecha polegająca na zachowywaniu dokładności i kompletności informacji i zasobów;
Niezaprzeczalność:	możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia.

II. ZASADY ZABEZPIECZANIA INFORMACJI

3. Przedstawione poniżej przepisy stanowią podstawę bezpieczeństwa wszelkich systemów CIS, w ramach których przetwarzane są EUCI. Szczegółowe wymogi dotyczące wdrażania tych przepisów są zdefiniowane w ramach polityk bezpieczeństwa w zakresie zabezpieczania informacji oraz w wytycznych dotyczących bezpieczeństwa.

Zarządzanie ryzykiem dla bezpieczeństwa

4. Zarządzanie ryzykiem dla bezpieczeństwa stanowi integralną część definiowania, rozwijania, obsługiwania i konserwacji CIS. Zarządzanie ryzykiem (ocena, zmniejszanie, akceptacja i powiadamianie) jest prowadzone jako interaktywny proces wspólnie przez przedstawicieli właścicieli systemu, organy odpowiedzialne za projekt, organy operacyjne oraz organy zatwierdzające bezpieczeństwo, w ramach sprawdzonego, przejrzystego i w pełni zrozumiałego procesu oceny ryzyka. Zakres stosowania CIS oraz jego zasobów jest jasno definiowany na początku procesu zarządzania ryzykiem.

5. Właściwe organy dokonują przeglądu potencjalnych zagrożeń dla CIS i posiadają aktualne i dokładne oceny zagrożeń, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat podatności na zagrożenia i dokonują okresowych przeglądów oceny podatności, aby dostosować się do zmieniających się technologii informatycznych (IT).

6. Celem zmniejszania ryzyka naruszenia zasad bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika, kosztami a szczątkowym ryzykiem naruszenia zasad bezpieczeństwa.

7. Szczególne wymogi, skala i stopień szczegółowości określone przez odpowiednie SAA do celów przyznania akredytacji CIS są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym poziomu klauzuli tajności EUCI przetwarzanych w danym CIS. Akredytacja obejmuje oficjalne oświadczenie o ryzyku szczątkowym oraz akceptację ryzyka szczątkowego przez odpowiedzialny organ.

Bezpieczeństwo w całym cyklu życia CIS

8. Zapewnianie bezpieczeństwa jest wymogiem obowiązującym w całym cyklu życia CIS, od jego uruchomienia do wycofania z użytkowania.

9. Dla każdego etapu cyklu życia CIS określana jest rola i interakcja każdego z podmiotów związanych z CIS w odniesieniu do jego bezpieczeństwa.

10. Wszystkie CIS wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacji poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia zabezpieczenia oraz sprawdzić, czy są one prawidłowo wdrożone, zintegrowane i skonfigurowane.

11. Oceny bezpieczeństwa, inspekcje i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji CIS, jak również przy pojawieniu się nadzwyczajnych okoliczności.

12. Dokumentacja bezpieczeństwa CIS ewoluuje podczas wszystkich etapów jego cyklu życia na zasadzie integralnej części procesu zmian i zarządzania konfiguracjami.

Dobre praktyki

13. SGR i państwa członkowskie współpracują, aby opracować dobre praktyki ochrony EUCI, które przetwarza się w ramach CIS. Wytyczne w zakresie dobrych praktyk zawierają techniczne, fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące CIS o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i podatności.

14. Ochrona EUCI przetwarzanych w ramach CIS opiera się na doświadczeniach podmiotów zaangażowanych w zabezpieczanie informacji, zarówno w UE, jak i poza nią.

15. Rozpowszechnianie, a następnie wdrażanie dobrych praktyk pomaga w osiągnięciu równoważnego poziomu zabezpieczenia różnych CIS, eksploatowanych przez SGR i państwa członkowskie, które przetwarzają EUCI.

Ochrona w głąb

16. Aby zmniejszyć ryzyko zagrażające CIS, wdrażany jest pakiet technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów ochrony. Poziomy te obejmują:

a) *Powstrzymywanie:* środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na CIS;

b) *Zapobieganie:* środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS;

c) *Wykrywanie:* środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS;

d) *Odporność:* środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów CIS, oraz na zapobieżenie dalszym szkodom; oraz

e) *Usuwanie skutków:* środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS.

Stopień rygorystyczności takich środków bezpieczeństwa ustalany jest na podstawie oceny ryzyka.

17. Właściwe organy dbają o to, by były w stanie reagować na incydenty, które mogą przekraczać granice poszczególnych organizacji i państw, koordynować reakcje i dzielić się informacjami o tych incydentach i związanym z nimi ryzyku (zdolności do reagowania na sytuacje nadzwyczajne w ramach systemów komputerowych).

Zasada minimalizmu i najmniejszych uprawnień

18. Aby zapobiec niepotrzebnemu ryzyku, stosowane są wyłącznie funkcje, urządzenia i usługi niezbędne do spełnienia wymogów operacyjnych.

19. Aby ograniczyć szkody wynikające z wypadków, błędów lub nieuprawnionego korzystania z zasobów CIS, użytkownicy CIS oraz procesy zautomatyzowane otrzymują wyłącznie taki dostęp i takie przywileje i upoważnienia, jakie są im niezbędne do wykonywania ich zadań.

20. Procedury rejestracji stosowane w razie konieczności w ramach CIS sprawdzane są jako element procedury akredytacji.

Świadomość zabezpieczania informacji

21. Świadomość ryzyka i dostępnych środków bezpieczeństwa stanowi pierwszą linię obrony bezpieczeństwa CIS. W szczególności wszyscy członkowie personelu związani z CIS na poszczególnych etapach jego cyklu życia, w tym użytkownicy, powinni zrozumieć:

a) że niedopatrzenia w zakresie bezpieczeństwa mogą znacznie zaszkodzić CIS;

b) potencjalne szkody, jakie mogą ponieść inne podmioty w związku z podłączeniem do systemów lub sieci i współzależnością; oraz

c) że osobiście ponoszą odpowiedzialność i są rozliczani za bezpieczeństwo CIS zgodnie z pełnionymi przez siebie funkcjami w tych systemach i procesach.

22. Aby zapewnić zrozumienie obowiązków związanych z bezpieczeństwem, wszyscy członkowie personelu związani z CIS, w tym wyższe kierownictwo i użytkownicy CIS, przechodzą obowiązkowe szkolenia mające na celu edukację i zdobycie wiedzy w zakresie zabezpieczania informacji.

Ocena i zatwierdzanie produktów służących bezpieczeństwu systemów informatycznych

23. Wymagany stopień zabezpieczenia, jaki zapewniają środki bezpieczeństwa, określony jako poziom zabezpieczenia, określa się zgodnie z wynikami procesu zarządzania ryzykiem i zgodnie z odpowiednimi politykami i wytycznymi dotyczącymi bezpieczeństwa.

24. Poziom zabezpieczenia sprawdzany jest przy użyciu uznanych na szczeblu międzynarodowym lub zatwierdzonych na szczeblu krajowym procesów i metod. Obejmują one przede wszystkim ocenę, kontrole i audyt.

25. Produkty kryptograficzne służące ochronie EUCI są oceniane i zatwierdzane przez krajowy CAA państwa członkowskiego.

26. Przed zaleceniem Radzie lub Sekretarzowi Generalnemu zatwierdzenia produktów kryptograficznych, zgodnie z art. 10 ust. 6, produkty te muszą uzyskać pozytywny wynik podczas zewnętrznej oceny dokonywanej przez wykwalifikowany organ oceny produktów kryptograficznych (AQUA) państwa członkowskiego, które nie jest zaangażowane w projektowanie ani wytwarzanie tego sprzętu. Wymagany stopień szczegółowości oceny zewnętrznej zależy od przewidywanego najwyższego poziomu klauzuli tajności EUCI, które mają być chronione za pomocą tych produktów. Rada zatwierdza politykę bezpieczeństwa dotyczącą oceny i zatwierdzania produktów kryptograficznych.

27. Jeżeli uzasadniają to określone względy operacyjne, Rada lub, w odpowiednich przypadkach, Sekretarz Generalny mogą znieść na zalecenie Komitetu ds. Bezpieczeństwa wymogi wynikające z pkt 25 lub 26 i udzielić tymczasowej akceptacji na dany okres zgodnie z procedurą określoną w art. 10 ust. 6.

28. AQUA jest organem ds. zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego, który na podstawie kryteriów ustalonych przez Radę otrzymał akredytację, aby przeprowadzić ocenę zewnętrzną produktów kryptograficznych służących ochronie EUCI.

29. Rada zatwierdza politykę bezpieczeństwa dotyczącą kwalifikowania i zatwierdzania niekryptograficznych produktów służących bezpieczeństwu systemów informatycznych.

Transmisja w strefie bezpieczeństwa

30. Niezależnie od przepisów niniejszej decyzji, gdy transmisja EUCI ogranicza się do stref bezpieczeństwa, można je dystrybuować w postaci niezaszyfrowanej lub zaszyfrować je na niższym poziomie na podstawie wyników procesu zarządzania ryzykiem i z zastrzeżeniem zatwierdzenia przez SAA.

Bezpieczne połączenia międzysystemowe CIS

31. Do celów niniejszej decyzji połączenie międzysystemowe oznacza bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy.

32. CIS traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niewzbudzający zaufania i stosuje środki ochrony, aby kontrolować wymianę informacji niejawnych.

33. Wszystkie połączenia międzysystemowe CIS z innym systemem informatycznym spełniają następujące podstawowe wymogi:

a) właściwe organy określają i zatwierdzają wymogi – biznesowe i operacyjne – dla takich połączeń;

b) połączenie międzysystemowe przechodzi proces zarządzania ryzykiem i akredytacji oraz wymaga zatwierdzenia przez właściwe organy akredytacji bezpieczeństwa; oraz

c) na granicach wszystkich CIS stosowane są usługi ochrony na granicy systemów (BPS).

34. Pomiędzy CIS posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach CIS zainstalowano w tym celu zatwierdzone BPS między CIS a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji i zatwierdzane przez właściwy SAA.

Gdy sieć niezabezpieczona lub publiczna wykorzystywana jest wyłącznie jako nośnik, a dane zostały zaszyfrowane przy wykorzystaniu produktu kryptograficznego zatwierdzonego zgodnie z art. 10, takiego połączenia nie uznaje się za połączenie międzysystemowe.

35. Bezpośrednie lub kaskadowe połączenie międzysystemowe CIS posiadającego akredytację do przetwarzania informacji o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET z siecią niezabezpieczoną lub publiczną jest zakazane.

Komputerowe nośniki informacji

36. Komputerowe nośniki informacji są niszczone zgodnie z procedurami zatwierdzonymi przez właściwy organ bezpieczeństwa.

37. Komputerowe nośniki informacji są ponownie używane, ich klauzula tajności może zostać obniżona lub zniesiona zgodnie z polityką bezpieczeństwa, którą należy ustalić na mocy art. 6 ust. 1.

Okoliczności nadzwyczajne

38. Niezależnie od przepisów niniejszej decyzji w okolicznościach nadzwyczajnych, takich jak zbliżający się lub trwający kryzys, konflikt, stan wojny, lub w wyjątkowych sytuacjach operacyjnych można stosować specjalne procedury opisane poniżej.

39. EUCI można przekazywać z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli tajności lub w postaci niezaszyfrowanej za zgodą właściwego organu, jeżeli wszelka zwłoka spowodowałaby szkody wyraźnie większe od szkód, które mogłoby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:

a) nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego lub też nie posiadają żadnego urządzenia szyfrującego; oraz

b) materiały niejawne nie mogą być dostarczone na czas w inny sposób.

40. Informacje niejawne przekazywane w okolicznościach przedstawionych w pkt 38 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 za pomocą innych środków bezzwłocznie powiadamiani o poziomie klauzuli tajności.

41. W przypadku stosowania przepisów pkt 38 należy następnie sporządzić sprawozdanie dla właściwych organów i Komitetu ds. Bezpieczeństwa.

III. FUNKCJE I ORGANY ZABEZPIECZANIA INFORMACJI

42. Państwa członkowskie i SGR otrzymują wymienione poniżej zadania dotyczące zabezpieczania informacji. Zadania te nie muszą być skupione w tych samych jednostkach organizacyjnych. Są one objęte oddzielnymi mandatami. Zadania te, oraz związana z nimi odpowiedzialność, mogą być jednak połączone lub zintegrowane w tej samej jednostce organizacyjnej lub też podzielone na różne jednostki organizacyjne, z zastrzeżeniem uniknięcia wewnętrznych konfliktów interesów lub zadań.

Organ ds. zabezpieczania informacji

43. Organ ds. zabezpieczania informacji (IAA) odpowiada za:

a) opracowywanie polityki bezpieczeństwa i wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji oraz za monitorowanie ich skuteczności i adekwatności;

b) zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;

c) zapewnianie, by środki zabezpieczania informacji wybrane do ochrony EUCI były zgodne z odpowiednimi politykami dotyczącymi kryteriów ich przydatności i wyboru;

d) zapewnianie, by wybór produktów kryptograficznych następował zgodnie z politykami dotyczącymi kryteriów ich przydatności i wyboru;

e) koordynowanie szkoleń i upowszechnianie wiedzy na temat zabezpieczania informacji;

f) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z polityką bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa w zakresie zabezpieczania informacji; oraz

g) zapewnianie odpowiedniej wiedzy fachowej na temat zabezpieczania informacji w podgrupie eksperckiej Komitetu ds. Bezpieczeństwa.

Organ ds. TEMPEST

44. Organ ds. TEMPEST (TA) odpowiada za zapewnienie zgodności CIS z politykami i wytycznymi TEMPEST. Zatwierdza on środki zaradcze TEMPEST dla instalacji i produktów służące temu, by w środowisku operacyjnym chronić EUCI do określonego poziomu klauzuli tajności.

Organ ds. zatwierdzania produktów kryptograficznych

45. Organ ds. zatwierdzania produktów kryptograficznych (CAA) odpowiada za zapewnienie zgodności produktów kryptograficznych z krajową polityką kryptograficzną lub polityką kryptograficzną Rady. Wydaje on zgodę na to, by dany produkt kryptograficzny w swoim środowisku operacyjnym chronił EUCI do określonego poziomu klauzuli tajności. Jeżeli chodzi o państwa członkowskie, CAA jest dodatkowo odpowiedzialny za ocenę produktów kryptograficznych.

Organ ds. dystrybucji produktów kryptograficznych

46. Organ ds. dystrybucji produktów kryptograficznych (CDA) odpowiada za:

a) zarządzanie materiałami kryptograficznymi UE i przyjęcie za nie odpowiedzialności;

b) zapewnianie stosowania odpowiednich procedur i stworzenia kanałów umożliwiających przyjmowanie odpowiedzialności za wszystkie materiały kryptograficzne UE, ich bezpieczne wykorzystywanie, przechowywanie i rozpowszechnianie; oraz

c) zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów.

Organ ds. akredytacji bezpieczeństwa

47. SAA jest w każdym systemie odpowiedzialny za:

a) zapewnianie zgodności CIS z odpowiednimi politykami bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, dostarczając poświadczenie zatwierdzenia CIS do celów przetwarzania EUCI do określonego poziomu klauzuli tajności w jego środowisku operacyjnym; w poświadczeniu określa się warunki akredytacji oraz kryteria, które muszą być spełnione, by konieczne było ponowne zatwierdzenie;

b) stworzenie procesu akredytacji bezpieczeństwa, zgodnie z odpowiednimi politykami, z wyraźnie określonymi warunkami zatwierdzenia CIS pod nadzorem tego organu;

c) określanie strategii akredytacji bezpieczeństwa przez ustalenie stopnia szczegółowości procedury akredytacji proporcjonalnego do wymaganego poziomu zabezpieczenia;

d) analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o zarządzaniu ryzykiem i o ryzyku szczątkowym, oświadczeń o szczególnych wymaganiach bezpieczeństwa systemu (zwanych dalej „SSRS"), dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu (zwanych dalej „SecOP"), jak również zapewnianie zgodności tej dokumentacji z polityką i przepisami bezpieczeństwa Rady;

e) sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań;

f) określanie wymogów bezpieczeństwa (np. poziomów sprawdzania pracowników) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS;

g) zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa CIS;

h) zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia CIS z innymi CIS; oraz

i) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z zarządzaniem ryzykiem dla bezpieczeństwa, w szczególności ryzykiem szczątkowym, jak również z warunkami i okolicznościami poświadczenia zatwierdzenia.

48. Organ ds. akredytacji bezpieczeństwa SGR jest odpowiedzialny za przyznawanie akredytacji wszystkim CIS działającym pod nadzorem SGR.

49. Odpowiedni SAA państwa członkowskiego jest odpowiedzialny za przyznawanie akredytacji CIS oraz jego częściom składowym działającym pod nadzorem danego państwa członkowskiego.

50. Wspólna rada ds. akredytacji bezpieczeństwa (SAB) jest odpowiedzialna za przyznawanie akredytacji CIS działającym pod nadzorem zarówno organu ds. akredytacji bezpieczeństwa SGR, jak i SAA państw członkowskich. W skład tej rady wchodzi po jednym przedstawicielu SAA z każdego państwa członkowskiego, a w jej obradach uczestniczy przedstawiciel SAA z Komisji. Inne podmioty posiadające połączenia z danym CIS są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

Obradom SAB przewodniczy przedstawiciel organu ds. akredytacji bezpieczeństwa SGR. SAB podejmuje decyzje na zasadzie konsensusu przedstawicieli SAA z instytucji, państw członkowskich i innych podmiotów posiadających połączenia z danym CIS. SAB sporządza okresowe sprawozdania ze swojej działalności i przedstawia je Komitetowi ds. Bezpieczeństwa oraz informuje komitet o wszystkich świadectwach akredytacji.

Operacyjny organ ds. zabezpieczania informacji

51. Operacyjny organ ds. zabezpieczania informacji odpowiada w każdym systemie za:

a) opracowanie dokumentacji bezpieczeństwa zgodnie z politykami bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza SSRS, w tym oświadczenia o ryzyku szczątkowym, SecOP i planu kryptograficznego w ramach procesu akredytacji CIS;

b) uczestnictwo w wyborze i testowaniu technicznych środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów, nadzorowanie ich wdrażania i zapewnianie, by były one w bezpieczny sposób instalowane, konfigurowane i konserwowane zgodnie z odpowiednią dokumentacją bezpieczeństwa;

c) uczestnictwo w wyborze środków bezpieczeństwa i urządzeń klasy TEMPEST, jeżeli jest to wymagane na podstawie SSRS, i zapewnianie, by były one w bezpieczny sposób instalowane i konserwowane we współpracy z TA;

d) monitorowanie wdrażania i stosowania SecOP, a w odpowiednich przypadkach zlecanie właścicielowi systemu operacyjnych obowiązków w zakresie bezpieczeństwa;

e) zarządzanie produktami kryptograficznymi i ich wykorzystywanie, zapewnianie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeżeli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych;

f) przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami SAA;

g) zapewnianie szkolenia w zakresie zabezpieczania informacji w odniesieniu do poszczególnych CIS;

h) wdrażanie środków bezpieczeństwa w odniesieniu do poszczególnych CIS i stosowanie tych środków.

ZAŁĄCZNIK V

BEZPIECZEŃSTWO PRZEMYSŁOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 11. Ustanawia on ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów prowadzących działalność gospodarczą lub inną podczas negocjacji poprzedzających zawarcie umowy oraz na wszystkich etapach cyklu życia umów niejawnych zawartych przez SGR.

2. Rada zatwierdza politykę bezpieczeństwa przemysłowego, w szczególności szczegółowe wymogi w odniesieniu do SBP, dokumentu określającego aspekty bezpieczeństwa (DOAB), wizyt, transmisji i przewożenia EUCI.

II. ELEMENTY DOTYCZĄCE BEZPIECZEŃSTWA W UMOWIE NIEJAWNEJ

Przewodnik nadawania klauzul (PNK)

3. Przed zamieszczeniem ogłoszenia o przetargu lub zawarciem umowy niejawnej, SGR, jako instytucja zamawiająca, określa klauzulę tajności wszelkich informacji, które należy dostarczyć oferentom i wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym celu SGR opracowuje PNK, który należy stosować podczas wykonywania umów.

4. Do określania klauzuli tajności różnych elementów umowy niejawnej zastosowanie mają następujące zasady:

   a) podczas opracowywania PNK, SGR uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę tajności nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie do celów umowy zatwierdził;

   b) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności któregokolwiek z jej elementów; oraz

   c) w odpowiednich przypadkach SGR działa w porozumieniu z KWB/WWB państw członkowskich lub jakimkolwiek innym właściwym organem bezpieczeństwa na wypadek jakichkolwiek zmian klauzul tajności informacji wytworzonych przez wykonawców lub przekazanych im podczas wykonywania umowy oraz w przypadku wprowadzania jakichkolwiek późniejszych zmian do PNK.

Dokument określający aspekty bezpieczeństwa (DOAB)

5. Wymogi bezpieczeństwa dotyczące poszczególnych umów opisane są w DOAB. DOAB w odpowiednich przypadkach zawiera PNK i stanowi integralną część umowy niejawnej lub niejawnej umowy o podwykonawstwo.

6. DOAB zawiera przepisy zobowiązujące wykonawcę lub podwykonawcę do przestrzegania minimalnych norm określonych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może stanowić wystarczający powód do rozwiązania umowy.

Instrukcje bezpieczeństwa programu/projektu (IBP)

7. W zależności od zakresu programów lub projektów obejmujących dostęp do EUCI, ich wykorzystywanie lub przechowywanie, organ wyznaczony do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa programu/projektu (IBP). IBP wymagają zatwierdzenia przez KWB/WWB państw członkowskich lub jakikolwiek inny właściwy organ bezpieczeństwa uczestniczący w programie/projekcie i mogą zawierać dodatkowe wymogi bezpieczeństwa.

III. ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (SBP)

8. SBP wydawane jest 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 prowadzący działalność gospodarczą lub inną jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET). Świadectwo to przedstawiane jest SGR, jako instytucji zamawiającej, przed dostarczeniem EUCI wykonawcy, podwykonawcy, potencjalnemu wykonawcy lub potencjalnemu podwykonawcy, lub umożliwieniem im dostępu do EUCI.

9. Przy wydawaniu SBP odpowiednia KWB lub WWB przynajmniej:

   a) ocenia integralność podmiotu prowadzącego działalność gospodarczą lub inną;

   b) ocenia własność, kontrolę lub możliwość wystąpienia niewłaściwego wpływu, który można uznać za ryzyko naruszenia zasad bezpieczeństwa;

c) ocenia, czy podmiot prowadzący działalność gospodarczą lub inną stworzył w obiekcie system bezpieczeństwa, który obejmuje wszystkie odpowiednie środki bezpieczeństwa niezbędne do ochrony informacji lub materiałów niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET zgodnie z wymogami określonymi w niniejszej decyzji;

d) ocenia, czy status bezpieczeństwa osobowego kadry zarządzającej, właścicieli i pracowników, którzy mają mieć dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, został ustalony zgodnie z wymogami określonymi w niniejszej decyzji;

e) ocenia, czy podmiot prowadzący działalność gospodarczą lub inną powołał pełnomocnika ochrony, który jest odpowiedzialny wobec kadry zarządzającej za egzekwowanie obowiązków dotyczących bezpieczeństwa w obrębie tego podmiotu.

10. W stosownych przypadkach SGR, jako instytucja zamawiająca, powiadamia odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o tym, że na etapie poprzedzającym zawarcie umowy lub do wykonywania umowy wymagane jest SBP. SBP lub PBO są wymagane na etapie poprzedzającym zawarcie umowy, jeżeli podczas składania ofert mają być dostarczone EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.

11. Instytucja zamawiająca nie zawiera umowy niejawnej z wybranym oferentem, zanim nie otrzyma od KWB/WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest ten wykonawca lub podwykonawca, potwierdzenia, że wydane zostało, jeśli istnieje taki wymóg, odpowiednie SBP.

12. KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa, który wydał SBP, powiadamiają SGR, jako instytucję zamawiającą, o wszelkich zmianach dotyczących SBP. W przypadku umowy o podwykonawstwo KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa są o tym informowane.

13. Cofnięcie SBP przez odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa stanowią dla SGR, jako instytucji zamawiającej, wystarczający powód do rozwiązania umowy niejawnej lub wykluczenia oferenta z postępowania.

IV. UMOWY NIEJAWNE I NIEJAWNE UMOWY O PODWYKONAWSTWO

14. Jeżeli EUCI przekazywane są oferentowi na etapie poprzedzającym zawarcie umowy, ogłoszenie przetargu zawiera przepis zobowiązujący oferenta, który nie złoży oferty lub który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.

15. Po zawarciu umowy niejawnej lub niejawnej umowy o podwykonawstwo SGR, jako instytucja zamawiająca, powiadamia KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa wykonawcy lub podwykonawcy o zawartych w tej umowie przepisach bezpieczeństwa.

16. W przypadku rozwiązania takich umów SGR, jako instytucja zamawiająca (lub, w odpowiednim przypadku, KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa w przypadku umowy o podwykonawstwo) niezwłocznie powiadamia o tym fakcie KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

17. Z reguły od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego EUCI po zakończeniu obowiązywania umowy niejawnej lub niejawnej umowy o podwykonawstwo.

18. W DOAB określa się szczególne przepisy dotyczące niszczenia EUCI podczas wykonywania umowy lub po zakończeniu jej obowiązywania.

19. Jeżeli wykonawca lub podwykonawca są upoważnieni do zachowania EUCI po zakończeniu obowiązywania umowy, nadal przestrzegają oni minimalnych norm zawartych w niniejszej decyzji i nadal chronią poufność EUCI.

20. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ogłoszeniu o przetargu oraz w umowie.

21. Przed zleceniem podwykonawstwa części umowy niejawnej wykonawca uzyskuje zgodę SGR jako instytucji zamawiającej. Nie można zawrzeć umowy o podwykonawstwo z podmiotami prowadzącymi działalność gospodarczą lub inną zarejestrowanymi w państwie niebędącym członkiem UE, które nie zawarło z UE umowy o bezpieczeństwie informacji.

22. Wykonawca odpowiada za zapewnienie zgodności wszystkich podejmowanych czynności podwykonawczych z minimalnymi normami określonymi w niniejszej decyzji i nie dostarcza EUCI podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej.

23. W odniesieniu do EUCI wytworzonych lub wykorzystywanych przez wykonawcę lub podwykonawcę prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

V. WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI

24. Jeżeli SGR, wykonawcy lub podwykonawcy niezbędny jest w związku z wykonaniem umowy niejawnej dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w swoich obiektach, organizowane są wizyty wraz z KWB/WWB lub jakimkolwiek innym właściwym organem bezpieczeństwa. Jednak w kontekście konkretnych projektów KWB/WWB mogą uzgodnić procedurę umożliwiającą bezpośrednie organizowanie wizyt.

25. Wszystkie osoby wizytujące posiadają odpowiednie PBO i podlegają zasadzie ograniczonego dostępu, co uprawnia je do dostępu do EUCI związanych z umową zawartą przez SGR.

26. Osobom wizytującym umożliwia się dostęp wyłącznie do EUCI związanych z celem wizyty.

VI. TRANSMISJA I PRZEWOŻENIE EUCI

27. Do transmisji EUCI drogą elektroniczną zastosowanie mają odpowiednie przepisy art. 10 i załącznika IV.

28. Do przewożenia EUCI zastosowanie mają odpowiednie przepisy załącznika III zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

29. Podczas transportu materiału niejawnego jako ładunku do określania zabezpieczeń stosuje się następujące zasady:

a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do ostatecznego miejsca przeznaczenia;

b) stopień ochrony, którym objęto przesyłkę określany jest według najwyższej klauzuli tajności materiału zawartego w przesyłce;

c) firmy dokonujące przewozu uzyskują SBP na stosownym poziomie. W takich przypadkach pracownicy zajmujący się przesyłką są odpowiednio sprawdzani zgodnie z załącznikiem I;

d) przed jakimkolwiek transgranicznym przemieszczeniem materiałów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, nadawca sporządza plan przewozu, który jest zatwierdzany przez odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa;

e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i kończą się tak szybko, jak pozwolą na to okoliczności;

f) 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.

VII. PRZEKAZYWANIE EUCI WYKONAWCOM ZNAJDUJĄCYM SIĘ W PAŃSTWACH TRZECICH

30. EUCI są przekazywane wykonawcom i podwykonawcom znajdującym się w państwach trzecich zgodnie ze środkami bezpieczeństwa uzgodnionymi przez SGR, jako instytucję zamawiającą, z KWB/WWB państwa trzeciego, w którym zarejestrowany jest wykonawca.

VIII. WYKORZYSTYWANIE I PRZECHOWYWANIE INFORMACJI NIEJAWNYCH O KLAUZULI TAJNOŚCI RESTREINT UE/EU RESTRICTED

31. W porozumieniu, odpowiednio, z KWB/WWB państwa członkowskiego, SGR, jako instytucja zamawiająca, jest upoważniony na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców, aby sprawdzić, czy wprowadzone zostały odpowiednie środki bezpieczeństwa mające zapewnić ochronę EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED zgodnie z wymogami umowy.

32. W zakresie, jaki jest wymagany na mocy krajowych przepisów ustawowych i wykonawczych, KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa są powiadamiane przez SGR, jako instytucję zamawiającą, o umowach niejawnych lub niejawnych umowach o podwykonawstwo zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED.

33. W przypadku umów zawartych przez SGR zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED od wykonawców, podwykonawców ani ich personelu nie wymaga się posiadania SBP ani PBO.

34. SGR, jako instytucja zamawiająca, analizuje odpowiedzi na ogłoszenia o przetargu w przypadku umów, które wymagają dostępu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, niezależnie od jakichkolwiek wymogów związanych z SBP lub PBO, które mogą być określone przez krajowe przepisy ustawowe i wykonawcze.

35. Warunki, na których wykonawca może zlecić podwykonawstwo, są zgodne z pkt 21.

36. Jeżeli umowa obejmuje przetwarzanie informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED w ramach CIS, który eksploatuje wykonawca, SGR, jako instytucja zamawiająca, zapewnia, aby umowa lub jakakolwiek umowa o podwykonawstwo określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji CIS, które są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników. Zakres akredytacji dla takiego CIS jest uzgadniany między instytucją zamawiającą a odpowiednią KWB/WWB.

ZAŁĄCZNIK VI

WYMIANA INFORMACJI NIEJAWNYCH Z PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 12.

II. RAMY REGULUJĄCE WYMIANĘ INFORMACJI NIEJAWNYCH

2. W przypadku gdy Rada stwierdza, że istnieje długoterminowa potrzeba wymiany informacji niejawnych:

— zawarta zostaje umowa o bezpieczeństwie informacji, lub

— zawarte zostaje porozumienie administracyjne,

zgodnie z art. 12 ust. 2 i sekcjami III i IV oraz na podstawie zalecenia Komitetu ds. Bezpieczeństwa.

3. Jeżeli EUCI wytworzone do celów operacji WPBiO mają zostać przekazane państwom trzecim lub organizacjom międzynarodowym uczestniczącym w takiej operacji, a nie istnieją żadne z ram prawnych, o których mowa w pkt 2, wymiana EUCI z uczestniczącym w operacji państwem trzecim lub organizacją międzynarodową regulowana jest, zgodnie z sekcją V, na mocy:

— umowy ramowej w sprawie udziału,

— umowy *ad hoc* w sprawie udziału, lub

— jeżeli nie zawarto żadnej z powyższych umów – porozumienia administracyjnego *ad hoc*.

4. Jeżeli brak jest ram prawnych, o których mowa w pkt 2 i 3, a podjęta zostaje decyzja o udostępnieniu EUCI państwu trzeciemu lub organizacji międzynarodowej w wyjątkowym trybie *ad hoc* zgodnie z sekcją VI, od tego państwa trzeciego lub organizacji międzynarodowej należy uzyskać pisemne zapewnienie, że wszelkie udostępnione im EUCI są chronione zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa określonymi w niniejszej decyzji.

III. UMOWY O BEZPIECZEŃSTWIE INFORMACJI

5. Umowy o bezpieczeństwie informacji ustanawiają podstawowe zasady i minimalne normy mające zastosowanie do wymiany informacji niejawnych między UE a państwem trzecim lub organizacją międzynarodową.

6. Umowy o bezpieczeństwie informacji przewidują techniczne uzgodnienia wykonawcze, dokonywane przez Biuro ds. Bezpieczeństwa SGR, ECSD oraz właściwy organ bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej. Takie uzgodnienia wykonawcze uwzględniają poziom ochrony przewidziany w przepisach, strukturach i procedurach dotyczących bezpieczeństwa istniejących w danym państwie trzecim lub danej organizacji międzynarodowej. Uzgodnienia te zatwierdzane są przez Komitet ds. Bezpieczeństwa.

7. Nie wymienia się żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w umowie o bezpieczeństwie informacji lub technicznych uzgodnieniach wykonawczych.

8. Umowy o bezpieczeństwie informacji przewidują, że przed wymianą informacji niejawnych na mocy umowy Biuro ds. Bezpieczeństwa SGR oraz ECSD zgodnie stwierdzają, że strona otrzymująca jest w stanie w odpowiedni sposób chronić i zabezpieczać informacje jej dostarczone.

9. Gdy Rada zawiera umowę o bezpieczeństwie informacji, dla każdej ze stron umowy zostaje wyznaczona kancelaria tajna, do której – jako głównego punktu – będą wpływać i z której będą przekazywane informacje niejawne.

10. Aby ocenić skuteczność przepisów, struktur i procedur dotyczących bezpieczeństwa w danym państwie trzecim lub organizacji międzynarodowej, Biuro ds. Bezpieczeństwa SGR wraz z ECSD oraz w porozumieniu z tym państwem trzecim lub organizacją międzynarodową przeprowadza wizyty oceniające. Wizyty takie przeprowadzane są zgodnie z odpowiednimi przepisami załącznika III i obejmują ocenę:

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 to, jaką najwyższą klauzulę tajności mogą mieć wymieniane informacje niejawne;

c) rzeczywiście stosowanych środków i procedur bezpieczeństwa; oraz

d) procedur prowadzenia postępowań sprawdzających odpowiadających klauzuli tajności EUCI, które mają być udostępniane.

11. Zespół przeprowadzający wizytę oceniającą w imieniu UE ocenia, czy obowiązujące w danym państwie trzecim lub organizacji międzynarodowej przepisy i procedury dotyczące bezpieczeństwa są odpowiednie do ochrony EUCI o określonym poziomie klauzuli tajności.

12. Wnioski z takich wizyt przedstawiane są w raporcie, na którego podstawie Komitet ds. Bezpieczeństwa określa najwyższą klauzulę tajności EUCI, które mogą być wymieniane z daną stroną trzecią w postaci papierowej, a w odpowiednich przypadkach –elektronicznej, a także wszelkie szczególne warunki wymiany informacji z tą stroną.

13. Należy dołożyć wszelkich starań, by przeprowadzić wizytę oceniającą zapewniającą pełną kontrolę bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej, zanim Komitet ds. Bezpieczeństwa zatwierdzi uzgodnienia wykonawcze, aby określić charakter i skuteczność funkcjonującego tam systemu bezpieczeństwa. Jeżeli jednak nie jest to możliwe, Komitet ds. Bezpieczeństwa otrzymuje od Biura ds. Bezpieczeństwa SGR możliwie najpełniejszy raport, sporządzony w oparciu o posiadane przez to biuro informacje, w którym komitet informowany jest o mających zastosowanie przepisach dotyczących bezpieczeństwa oraz o sposobie organizacji kwestii bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej.

14. Komitet ds. Bezpieczeństwa może zdecydować, że w oczekiwaniu na analizę wyników wizyty oceniającej nie można udostępnić żadnych EUCI lub można udostępnić te informacje tylko do określonego poziomu klauzuli tajności; komitet może też określić inne szczególne warunki dotyczące udostępniania EUCI danemu państwu trzeciemu lub danej organizacji międzynarodowej. Biuro ds. Bezpieczeństwa SGR powiadamia o tym dane państwo trzecie lub daną organizację międzynarodową.

15. Biuro ds. Bezpieczeństwa SGR, działając w porozumieniu z danym państwem trzecim lub daną organizacją międzynarodową, w regularnych odstępach czasu przeprowadza kolejne wizyty oceniające, aby sprawdzić, czy istniejące uzgodnienia nadal odpowiadają ustalonym minimalnym normom.

16. Po wejściu w życie umowy o bezpieczeństwie informacji i rozpoczęciu wymiany informacji niejawnych z danym państwem trzecim lub daną organizacją międzynarodową Komitet ds. Bezpieczeństwa może zdecydować o zmianie najwyższej klauzuli tajności EUCI, które mogą być wymieniane w postaci papierowej lub drogą elektroniczną, w szczególności w wyniku jednej z kolejnych wizyt oceniających.

IV. POROZUMIENIA ADMINISTRACYJNE

17. Jeżeli istnieje długoterminowa potrzeba wymiany z państwem trzecim lub organizacją międzynarodową informacji niejawnych o klauzuli tajności z reguły nie wyższej niż RESTREINT UE/EU RESTRICTED i jeżeli Komitet ds. Bezpieczeństwa ustalił, że dana strona nie dysponuje wystarczająco rozwiniętym systemem bezpieczeństwa, tak aby było możliwe zawarcie umowy o bezpieczeństwie informacji, Sekretarz Generalny może, z zastrzeżeniem zatwierdzenia przez Radę, zawrzeć porozumienie administracyjne z odpowiednimi organami danego państwa trzeciego lub organizacji międzynarodowej.

18. Jeżeli z pilnych przyczyn operacyjnych należy szybko utworzyć ramy prawne wymiany informacji niejawnych, Rada może wyjątkowo zdecydować o zawarciu porozumienia administracyjnego dotyczącego wymiany informacji o wyższej klauzuli tajności.

19. Porozumienia administracyjne co do zasady przyjmują postać wymiany listów.

20. Przed faktycznym udostępnieniem EUCI danemu państwu trzeciemu lub danej organizacji międzynarodowej przeprowadzana jest wizyta oceniająca, o której mowa w pkt 10, a raport przekazywany jest Komitetowi ds. Bezpieczeństwa, który ocenia go jako zadowalający. Jeżeli jednak istnieją wyjątkowe powody pilnej wymiany informacji niejawnych, na które to powody zwraca się uwagę Rady, EUCI mogą być udostępniane, pod warunkiem że dołoży się wszelkich starań, aby przeprowadzić taką wizytę oceniającą jak najszybciej.

21. Nie wymienia się żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w porozumieniu administracyjnym.

V. WYMIANA INFORMACJI NIEJAWNYCH W KONTEKŚCIE OPERACJI WPBiO

22. Umowy ramowe w sprawie udziału regulują uczestnictwo państw trzecich lub organizacji międzynarodowych w operacjach WPBiO. Umowy takie zawierają przepisy o udostępnianiu EUCI wytwarzanych do celów operacji WPBiO uczestniczącym w nich państwom trzecim lub organizacjom międzynarodowym. Najwyższym poziomem klauzuli tajności EUCI, które mogą być wymieniane, jest RESTREINT UE/EU RESTRICTED w przypadku operacji cywilnych WPBiO oraz CONFIDENTIEL UE/EUCONFIDENTIAL w przypadku operacji wojskowych WPBiO, chyba że inaczej określono we wspólnym działaniu ustanawiającym każdą z operacji WPBiO.

23. Umowy *ad hoc* w sprawie udziału w konkretnej operacji WPBiO zawierają przepisy o udostępnianiu EUCI wytwarzanych do celów tej operacji uczestniczącemu w niej państwu trzeciemu lub organizacji międzynarodowej. Najwyższym poziomem klauzuli tajności EUCI, które mogą być wymieniane, jest RESTREINT UE/EU RESTRICTED w przypadku operacji cywilnych WPBiO oraz CONFIDENTIEL UE/EUCONFIDENTIAL w przypadku operacji wojskowych WPBiO, chyba że inaczej określono w decyzji ustanawiającej każdą z operacji WPBiO.

24. Porozumienia administracyjne *ad hoc* dotyczące uczestnictwa państwa trzeciego lub organizacji międzynarodowej w konkretnej operacji WPBiO mogą obejmować m.in. udostępnianie temu państwu trzeciemu lub tej organizacji międzynarodowej EUCI wytworzonych do celów tej operacji. Takie porozumienia administracyjne *ad hoc* są zawierane zgodnie z procedurami określonymi w sekcji IV pkt 17 i 18. Najwyższym poziomem klauzuli tajności EUCI, które mogą być wymieniane, jest RESTREINT UE/EU RESTRICTED w przypadku operacji cywilnych WPBiO oraz CONFIDENTIEL UE/EUCONFIDENTIAL w przypadku operacji wojskowych WPBiO, chyba że inaczej określano w decyzji ustanawiającej każdą z operacji WPBiO.

25. Przed wdrożeniem przepisów w sprawie udostępniania EUCI na warunkach określonych w pkt 22, 23 i 24 nie są wymagane uzgodnienia wykonawcze ani wizyty oceniające.

26. Jeżeli państwo przyjmujące, na którego terytorium prowadzona jest operacja WPBiO, nie zawarło umowy o bezpieczeństwie informacji ani porozumienia administracyjnego z UE w zakresie wymiany informacji niejawnych, w przypadku konkretnej i natychmiastowej potrzeby operacyjnej można zawrzeć porozumienie administracyjne *ad hoc*. Możliwość ta przewidziana jest w decyzji ustanawiającej operację WPBiO. EUCI udostępnione w tych okolicznościach ograniczone są do informacji wytworzonych do celów operacji WPBiO i mają klauzulę tajności nie wyższą niż RESTREINT UE/EU RESTRICTED. Na mocy takiego porozumienia administracyjnego *ad hoc* państwo przyjmujące podejmuje się ochrony EUCI zgodnie z minimalnymi normami, które nie mogą być mniej rygorystyczne niż normy określone w niniejszej decyzji.

27. Przepisy dotyczące informacji niejawnych, które mają być zawarte w umowach ramowych w sprawie udziału, umowach *ad hoc* w sprawie udziału i porozumieniach administracyjnych *ad hoc*, o których mowa w pkt 22–24, przewidują, że dane państwo trzecie lub organizacja międzynarodowa zapewniają, by jego/jej personel oddelegowany do jakiejkolwiek operacji chronił EUCI zgodnie z przepisami bezpieczeństwa Rady i z dalszymi wytycznymi wydanymi przez właściwe organy, w tym strukturę dowodzenia operacji.

28. Jeżeli uczestniczące w operacji państwo trzecie lub organizacja międzynarodowa zawrze następnie z UE umowę o bezpieczeństwie informacji, zastępuje ona wszelkie umowy ramowe w sprawie udziału, umowy *ad hoc* w sprawie udziału i porozumienia administracyjne *ad hoc* związane z wymianą EUCI i ich wykorzystywaniem.

29. Nie zezwala się na wymianę z państwem trzecim lub organizacją międzynarodową EUCI drogą elektroniczną na mocy umowy ramowej w sprawie udziału, umowy *ad hoc* w sprawie udziału i porozumienia administracyjnego *ad hoc*, o ile nie jest to wyraźnie przewidziane w tej umowie lub w tym porozumieniu.

30. EUCI wytworzone do celów operacji WPBiO mogą być ujawnione personelowi oddelegowanemu do tej operacji przez państwa trzecie lub organizacje międzynarodowe zgodnie z pkt 22–29. Upoważniając taki personel do dostępu do EUCI w obiektach lub w ramach CIS operacji WPBiO, stosuje się środki (w tym rejestrację ujawnianych EUCI) służące złagodzeniu ryzyka utraty lub narażenia na szwank bezpieczeństwa informacji. Środki te są określane w odpowiednich dokumentach dotyczących planowania lub misji.

VI. WYJĄTKOWE UDOSTĘPNIANIE EUCI *AD HOC*

31. Jeżeli nie ustanowiono ram prawnych zgodnie z sekcjami III–V, a Rada lub jeden z jej organów przygotowawczych stwierdza, że istnieje wyjątkowa potrzeba udostępnienia EUCI państwu trzeciemu lub organizacji międzynarodowej, SGR:

a) w miarę możliwości sprawdza z organami bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej, czy ich przepisy, struktury i procedury dotyczące bezpieczeństwa gwarantują ochronę udostępnianych EUCI zgodnie z normami nie mniej rygorystycznymi niż normy określone w niniejszej decyzji;

b) zwraca się do Komitetu ds. Bezpieczeństwa, by na podstawie dostępnych informacji wydał zalecenie dotyczące zaufania, jakie można mieć do przepisów, struktur i procedur dotyczących bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, którym mają zostać udostępnione EUCI.

32. Jeżeli Komitet ds. Bezpieczeństwa wyda zalecenie, by udostępnić EUCI, sprawa zostaje przekazana Komitetowi Stałych Przedstawicieli (COREPER), który podejmuje decyzję o udostępnieniu tych informacji.

33. Jeżeli Komitet ds. Bezpieczeństwa wyda zalecenie, by nie udostępniać EUCI:

a) w sprawach odnoszących się do WPZiB/WPBiO Komitet Polityczny i Bezpieczeństwa omawia tę kwestię i formułuje zalecenie dotyczące decyzji COREPER-u;

b) we wszystkich innych sprawach COREPER omawia tę kwestię i podejmuje decyzję.

34. We właściwych przypadkach i po uzyskaniu wcześniej pisemnej zgody wytwórcy COREPER może postanowić o udostępnieniu informacji niejawnych wyłącznie częściowo lub wyłącznie pod warunkiem uprzedniego obniżenia lub zniesienia klauzuli tajności lub też pod warunkiem, że informacje, które mają zostać udostępnione, przygotowane zostaną bez odniesienia do źródła lub pierwotnej klauzuli tajności UE.

35. W następstwie decyzji o udostępnieniu EUCI, SGR przekazuje dany dokument, który jest opatrzony oznaczeniem dotyczącym możliwości jego udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym zostaje udostępniony. 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 normami określonymi w niniejszej decyzji.

VII. UPOWAŻNIENIE DO UDOSTĘPNIANIA EUCI PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

36. Jeżeli istnieją ramy prawne wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową zgodnie z pkt 2, Rada podejmuje decyzję upoważniającą Sekretarza Generalnego do udostępniania EUCI temu państwu trzeciemu lub organizacji międzynarodowej, z zachowaniem zasady uzyskania zgody wytwórcy.

37. Jeżeli istnieją ramy prawne wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową zgodnie z pkt 3, Sekretarz Generalny upoważniony jest do udostępniania EUCI zgodnie ze wspólnym działaniem ustanawiającym daną operację WPBiO oraz z zachowaniem zasady uzyskania zgody wytwórcy.

38. Sekretarz Generalny może przenieść takie upoważnienie na urzędników wysokiego szczebla w SGR lub inne osoby, których jest zwierzchnikiem.

Dodatki

Dodatek A

DEFINICJE

Do celów niniejszej decyzji zastosowanie mają następujące definicje:

„Akredytacja" oznacza proces prowadzący do formalnego stwierdzenia przez organ ds. akredytacji bezpieczeństwa (SAA), że określony system jest zatwierdzony do celów działania na zdefiniowanym poziomie klauzuli tajności, w konkretnym trybie bezpiecznej pracy systemu w swoim środowisku operacyjnym oraz na poziomie ryzyka możliwym do zaakceptowania, przy założeniu, że wdrożony został zatwierdzony zestaw technicznych, fizycznych, organizacyjnych i proceduralnych środków bezpieczeństwa;

„Bezpieczeństwo fizyczne" – zob. art. 8 ust. 1;

„Bezpieczeństwo osobowe" – zob. art. 7 ust. 1;

„Bezpieczeństwo przemysłowe" – zob. art. 11 ust. 1;

„Cykl życia CIS" oznacza cały okres istnienia CIS, który obejmuje powstanie pomysłu, opracowanie koncepcji, zaplanowanie, analizę wymogów, zaprojektowanie, utworzenie, testowanie, wdrożenie, działanie, konserwację i wycofanie z działania;

„Dokument określający aspekty bezpieczeństwa" (DOAB) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część jakiejkolwiek umowy niejawnej obejmującej dostęp do EUCI lub ich wytwarzanie, określający wymogi bezpieczeństwa lub wskazujący te elementy umowy, których bezpieczeństwo wymaga ochrony;

„Dokument" oznacza każdą utrwaloną informację, bez względu na jej formę fizyczną lub cechy charakterystyczne;

„Informacje niejawne UE" (EUCI) – zob. art. 2 ust. 1;

„Instrukcje bezpieczeństwa programu/projektu" (IBP) oznaczają wykaz procedur bezpieczeństwa stosowanych do określonego programu/projektu w celu ujednolicenia procedur bezpieczeństwa. Instrukcje mogą być zmieniane podczas trwania programu/projektu;

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

„Materiały" oznaczają jakikolwiek dokument lub dowolne urządzenia lub sprzęt, już wytworzone lub będące w trakcie wytwarzania;

„Niejawna umowa o podwykonawstwo" oznacza umowę zawieraną przez wykonawcę SGR z innym wykonawcą (tj. podwykonawcą) na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„Obniżenie klauzuli tajności" oznacza obniżenie poziomu klauzuli tajności;

„Ochrona w głąb" oznacza stosowanie pakietu środków bezpieczeństwa o różnych poziomach ochrony;

„Operacja WPBiO" oznacza wojskową lub cywilną operację zarządzania kryzysowego prowadzoną na mocy tytułu V rozdział 2 TUE;

„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;

„Podmiot prowadzący działalność gospodarczą lub inną" oznacza podmiot zajmujący się dostawą towarów, wykonywaniem robót lub świadczeniem usług; może to być podmiot prowadzący działalność gospodarczą, handlową, usługową, naukową, badawczą, edukacyjną lub rozwojową lub osoba prowadząca własną działalność;

„Połączenie międzysystemowe" – zob. załącznik IV pkt 31;

„Posiadacz" oznacza osobę posiadającą odpowiednie uprawnienia i spełniającą zasadę ograniczonego dostępu, znajdującą się w posiadaniu EUCI i w związku z tym odpowiedzialną za ich ochronę;

„Postępowanie sprawdzające" oznacza procedury sprawdzające przeprowadzane przez właściwy organ danego państwa członkowskiego zgodnie z jego przepisami ustawowymi i wykonawczymi w celu uzyskania pewności, że nie istnieją żadne niekorzystne okoliczności, które mogłyby stanowić przeszkodę w wydaniu danej osobie krajowego PBO lub PBO UE do dostępu do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej);

„Poświadczenie bezpieczeństwa osobowego" (PBO) oznacza jedno lub oba z poniższych:

— „poświadczenie bezpieczeństwa osobowego UE" (PBO UE) do dostępu do EUCI oznacza upoważnienie dokonane przez organ powołujący SGR zgodnie z niniejszą decyzją po przeprowadzeniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w którym to upoważnieniu poświadcza się, że danej osobie można w określonym terminie udzielać dostępu do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej), pod warunkiem że stwierdzono, iż osoba ta spełnia zasadę ograniczonego dostępu; o takiej osobie mówi się, że została „odpowiednio sprawdzona",

— „krajowe poświadczenie bezpieczeństwa osobowego" (krajowe PBO) do dostępu do EUCI oznacza poświadczenie właściwego organu państwa członkowskiego wydawane po przeprowadzeniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w którym to poświadczeniu stwierdza się, że danej osobie można w określonym terminie udzielać dostępu do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej), pod warunkiem że stwierdzono, iż osoba ta spełnia zasadę ograniczonego dostępu; o takiej osobie mówi się, że została „odpowiednio sprawdzona";

„Proces zarządzania ryzykiem dla bezpieczeństwa" oznacza cały proces określania, kontrolowania i minimalizacji związanych z ryzykiem wydarzeń, które mogą wpłynąć na bezpieczeństwo danej organizacji lub jakiegokolwiek systemu przez nią używanego. Obejmuje on wszystkie działania związane z ryzykiem, w tym ocenę, zmniejszanie, akceptację i powiadamianie;

„Przewodnik nadawania klauzul" (PNK) oznacza dokument opisujący niejawne elementy programu lub umowy i określający mające zastosowanie poziomy klauzul tajności. PNK może być rozszerzany podczas trwania programu lub umowy, a klauzule tajności dla części informacji mogą zostać zmienione lub obniżone; jeżeli PNK jest opracowany, to powinien być częścią dokumentu określającego aspekty bezpieczeństwa;

„Rejestracja" – zob. załącznik III pkt 18;

„Ryzyko szczątkowe" oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa, przy założeniu, że nie przeciwdziała się wszystkim zagrożeniom i że nie każdą podatność można wyeliminować;

„Ryzyko" oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu, z którego korzysta, i tym samym spowoduje szkody dla tej organizacji i jej materialnych lub niematerialnych zasobów. Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków.

— „Akceptacja ryzyka" jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

— „Ocena ryzyka" polega na określaniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

— „Powiadamianie 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 nich organom operacyjnym;

— „Zmniejszanie ryzyka" polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych), przenoszeniu lub monitorowaniu ryzyka;

„System teleinformatyczny" (CIS) – zob. art. 10 ust. 2;

„Świadectwo bezpieczeństwa przemysłowego" (SBP) oznacza stwierdzenie przez KWB lub WWB w wyniku procedur administracyjnych, że z punktu widzenia bezpieczeństwa dany podmiot jest w stanie zapewnić właściwą ochronę EUCI do określonego poziomu klauzuli tajności oraz że jego pracownicy, którym niezbędny jest dostęp do EUCI, zostali odpowiednio sprawdzeni oraz poinformowani o odpowiednich wymogach bezpieczeństwa niezbędnych do uzyskania dostępu do EUCI i do ochrony EUCI;

„TEMPEST" oznacza sprawdzenie, analizę i kontrolę emisji elektromagnetycznych umożliwiających przechwycenie danych oraz środki służące tłumieniu takich emisji;

„Tryb bezpiecznej pracy systemu" oznacza określenie warunków działania CIS na podstawie klauzul tajności informacji przetwarzanych oraz poziomów poświadczeń jego użytkowników, ich formalnych zatwierdzeń dostępu oraz zasady ograniczonego dostępu. Istnieją cztery tryby działania, jeżeli chodzi o przetwarzanie informacji niejawnych lub ich transmisję: tryb dedykowany, tryb systemowo-podwyższony, tryb zastrzeżony i tryb wielopoziomowy;

— „Tryb dedykowany" oznacza tryb pracy systemu, w którym wszystkie osoby posiadające dostęp do CIS są sprawdzane do celów dostępu do informacji o najwyższej klauzuli tajności, którą mają informacje przetwarzane w ramach CIS, oraz spełniają zasadę ograniczonego dostępu do wszystkich informacji przetwarzanych w ramach tego CIS,

— „Tryb systemowo-podwyższony" oznacza tryb prac systemu, w którym wszystkie osoby posiadające dostęp do CIS są sprawdzane do celów dostępu do informacji o najwyższym poziomie klauzuli tajności, którą mają informacje przetwarzane w ramach CIS, lecz nie wszystkie osoby posiadające dostęp do CIS spełniają zasadę ograniczonego dostępu do informacji przetwarzanych w ramach tego CIS; zgoda na dostęp do informacji może być udzielona przez określoną osobę,

— „Tryb zastrzeżony" oznacza tryb pracy systemu, w którym wszystkie osoby posiadające dostęp do CIS są sprawdzane do celów dostępu do informacji o najwyższym poziomie klauzuli tajności, którą mają informacje przetwarzane w ramach CIS, lecz nie wszystkie osoby posiadające dostęp do CIS posiadają formalne upoważnienie do dostępu do wszystkich informacji przetwarzanych w ramach tego CIS; formalne upoważnienie wymaga formalnego centralnego zarządzania kontrolą dostępu w odróżnieniu od prawa określonej osoby do udzielenia dostępu,

— „Tryb wielopoziomowy" oznacza tryb pracy systemu, w którym nie wszystkie osoby posiadające dostęp do CIS są sprawdzane do celów dostępu do informacji o najwyższym poziomie klauzuli tajności, którą mają informacje przetwarzane w ramach CIS, i nie wszystkie osoby posiadające dostęp do CIS spełniają zasadę ograniczonego dostępu do informacji przetwarzanych w ramach tego CIS;

„Umowa niejawna" oznacza umowę zawieraną przez SGR z wykonawcą na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„Wykonawca" oznacza osobę fizyczną lub prawną posiadającą zdolność prawną do zawierania umów;

„Wykorzystywanie/przetwarzanie" EUCI oznacza wszelkie możliwe działania, którym mogą podlegać EUCI na wszystkich etapach ich cyklu życia. Pojęcie to obejmuje wytwarzanie tych informacji, ich przetwarzanie, przewożenie, obniżenie klauzuli tajności, zniesienie klauzuli tajności oraz niszczenie. W przypadku CIS obejmuje ono także gromadzenie informacji, ich przedstawianie, transmisję i przechowywanie;

„Wytwórca" oznacza instytucję, agencję lub organ UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, pod nadzorem której wytworzono informacje niejawne lub wprowadzono je do struktur UE;

„Wyznaczona władza bezpieczeństwa" (WWB) oznacza organ podporządkowany krajowej władzy bezpieczeństwa (KWB) państwa członkowskiego, odpowiedzialny za informowanie podmiotów prowadzących działalność gospodarczą lub inną o krajowej polityce w zakresie wszelkich kwestii związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w ich wdrażaniu. Zadania WWB mogą być wykonywane przez KWB lub jakiekolwiek inny właściwy organ;

„Zabezpieczanie informacji" – zob. art. 10 ust. 1;

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

„Zarządzanie informacjami niejawnymi" – zob. art. 9 ust. 1;

„Zasoby" oznaczają wszystkie elementy, które mają wartość dla danej organizacji, prowadzenia przez nią działań i ich ciągłości, w tym zasoby informacyjne, które wspierają misję organizacji;

„Zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" (ZPBO) oznacza wydane przez właściwy organ zaświadczenie potwierdzające, że dana osoba została odpowiednio sprawdzona i posiada ważne krajowe PBO lub PBO UE, oraz określające poziom klauzuli tajności EUCI, do których osoba ta może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), okres ważności danego PBO oraz okres ważności samego zaświadczenia;

„Zniesienie klauzuli tajności" oznacza zniesienie jakiejkolwiek klauzuli tajności.

Dodatek B

ODPOWIEDNIKI KLAUZUL TAJNOŚCI

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU 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
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-Ogħla 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
Rumunia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
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	Top Secret	Secret	Confidential	Restricted

([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.

Dodatek C

WYKAZ KRAJOWYCH WŁADZ BEZPIECZEŃSTWA (KWB)

BELGIA
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. sekretariatu: + 32/2/5014542
Faks + 32/2/5014596
E-mail: nvo-ans@diplobel.fed.be

DANIA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel. + 45/33/148888
Faks + 45/33/430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel. + 45/33/325566
Faks + 45/33/931320

BUŁGARIA
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel. + 359/2/9215911
Faks + 359/2/9873750
E-mail: dksi@government.bg
Strona internetowa: www.dksi.bg

NIEMCY
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101D
11014 Berlin

Tel. + 49/30/186810
Faks + 49/30/186811441
E-mail: oesIII3@bmi.bund.de

REPUBLIKA CZESKA
Národní bezpečnostní úřad
(National Security Authority)
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

ESTONIA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel. +372/7170113, +372/7170117
Faks +372/7170213
E-mail: nsa@kmin.ee

IRLANDIA
National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2 Irlandia

Tel. + 353/1/ 4780822
Faks + 353/1/ 40829 59

HISZPANIA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel. + 34/91/372 5000
Faks + 34/91/372 5808
E-mail: nsa-sp@areatec.com

GRECJA
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: + 30/210/6572045(ώρες γραφείου)
+ 30/210/6572009 (ώρες γραφείου)
Φαξ: + 30/210/65362 79
+ 30/210/65776 12

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens

Tel. + 30/210/6572045
+ 30/210/6572009
Faks + 30/210/65362 79
+ 30/210/65776 12

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. + 33/1/71758177
Faks + 33/1/717582 00

WŁOCHY
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tel. + 39/06/611742 66
Faks + 39/06/48852 73

CYPR
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: + 357/22/807569, + 357/22/8076 43,
+ 357/22/807764
Τηλεομοιότυπο: + 357/22/302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tel. + 357/22/807569, + 357/22/8076 43,
+357/22/807764
Faks + 357/22/302351
E-mail: cynsa@mod.gov.cy

LUKSEMBURG
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tel. + 352/247822 10 central
+ 352/247822 53direct
Faks + 352/247822 43

WĘGRY
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tel. + 361/346 96 52
Faks + 361/346 96 58
E-mail: nbf@nbf.hu
Strona internetowa: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
Valletta

Tel. + 356/21249844
Faks + 356/2569 5321

ŁOTWA
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
1001 Riga

Tel. +371/6702 5418
Faks +371/6702 5454
Email: ndi@sab.gov.lv

LITWA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Co-ordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
01110 Vilnius

Tel. + 370/5/266 32 01,
+370/5/266 32 02
Faks + 370/5/266 32 00
E-mail: nsa@vsd.lt

NIDERLANDY
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel. + 31/70/3204400
Faks + 31/70/3200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel. + 31/70/3187060
Faks + 31/70/3187522

AUSTRIA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tel. + 43/1/531152594
Faks + 43/1/5311526 15
E-mail: ISK@bka.gv.at

POLSKA
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
Ul. Rakowiecka 2A
00-993 Warszawa

Tel. + 48/22/5857360
Faks + 48/22/5858509
E-mail: nsa@abw.gov.pl
Strona internetowa: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Ul. Oczki 1
02-007 Warszawa

Tel. + 48/22/68412 47
Faks + 48/22/6841076
E-mail: skw@skw.gov.pl

RUMUNIA
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest

Tel. + 40/21/ 2245830
Faks + 40/21/ 2240714
E-mail: nsa.romania@nsa.ro
Strona internetowa: www.orniss.ro

PORTUGALIA
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel. +351/ 213031710
Faks +351/ 213031711

SŁOWENIA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel. + 386/1/4781390
Faks + 386/1/4781399

SŁOWACJA
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel. + 421/2/6869 2314
Faks + 421/2/6382 4005
Strona internetowa: www.nbusr.sk

SZWECJA
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
10339 Stockholm

Tel. + 46/8/4051000
Faks + 46/8/7231176
E-mail: ud-nsa@foreign.ministry.se

FINLANDIA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
00023Government

Tel. 1 + 358/9/16056487
Tel. 2: +358/9/16056484
Fax: + 358/9/16055140
E-mail: NSA@formin.fi

ZJEDNOCZONE KRÓLESTWO
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Tel. 1: + 44/20/72765649
Tel. 2: + 44/20/72765497
Faks + 44/20/72765649
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Dodatek D

WYKAZ SKRÓTÓW

Akronim	Znaczenie
AQUA	Organ oceny produktów kryptograficznych
BPS	Usługi ochrony na granicy systemów
CAA	Organ ds. zatwierdzania produktów kryptograficznych
CCTV	Telewizja przemysłowa
CDA	Organ ds. dystrybucji produktów kryptograficznych
CIS	System teleinformatyczny przetwarzający EUCI
COREPER	Komitet Stałych Przedstawicieli
DOAB	Dokument określający aspekty bezpieczeństwa
ECSD	Dyrekcja ds. bezpieczeństwa Komisji Europejskiej
EUCI	Informacje niejawne UE
IAA	Organ ds. zabezpieczania informacji
IBP	Instrukcje bezpieczeństwa programu/projektu
IT	Technologie informatyczne
KWB	Krajowa władza bezpieczeństwa
PBO	Poświadczenie bezpieczeństwa osobowego
PNK	Przewodnik nadawania klauzul
SAA	Organ ds. akredytacji bezpieczeństwa
SAB	Wspólna rada ds. akredytacji bezpieczeństwa
SBP	Świadectwo bezpieczeństwa przemysłowego
SecOP	Procedury bezpiecznej eksploatacji systemu
SGR	Sekretariat Generalny Rady
SPUE	Specjalny przedstawiciel UE
SSRS	Szczególne wymagania bezpieczeństwa systemu
SSWiN	System sygnalizacji włamania i napadu
TA	Organ ds. TEMPEST
WPBiO	Wspólna polityka bezpieczeństwa i obrony
WPZiB	Wspólna polityka zagraniczna i bezpieczeństwa
WWB	Wyznaczona władza bezpieczeństwa
ZPBO	Zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego