DECYZJA KOMISJI (UE, Euratom) 2019/1963

z dnia 17 października 2019 r.

ustanawiająca przepisy wykonawcze dotyczące bezpieczeństwa przemysłowego w odniesieniu do niejawnych zamówień publicznych

KOMISJA EUROPEJSKA,

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

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

uwzględniając decyzję Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji ([1]),

uwzględniając decyzję Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE ([2]),

uwzględniając decyzję Komisji (UE, Euratom) 2017/46 z dnia 10 stycznia 2017 r. w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej ([3]),

po konsultacji z Grupą Ekspertów ds. Bezpieczeństwa Komisji, zgodnie z art. 41 ust. 5 decyzji (UE, Euratom) 2015/444,

a także mając na uwadze, co następuje:

(1) Art. 41, 42, 47 i 48 decyzji (UE, Euratom) 2015/444 stanowią, że w przepisach wykonawczych w zakresie bezpieczeństwa przemysłowego, regulujących kwestie takie jak procedura przetargowa, zawieranie umów niejawnych, świadectwa bezpieczeństwa przemysłowego, poświadczenia bezpieczeństwa osobowego, wizyty, transmisja i przemieszczanie informacji niejawnych UE (EUCI), mają zostać ustanowione bardziej szczegółowe przepisy w celu uzupełnienia i wsparcia rozdziału 6 decyzji.

(2) Decyzji (UE, Euratom) 2015/444 stanowi, że realizacja umów niejawnych musi odbywać się w ścisłej współpracy z krajową władzą bezpieczeństwa, wyznaczoną władzą bezpieczeństwa lub dowolnym innym właściwym organem danych państw członkowskich. Państwa członkowskie uzgodniły, że zapewnią, aby podmioty podlegające ich jurysdykcji i mogące otrzymywać lub tworzyć informacje niejawne pochodzące z Komisji były odpowiednio sprawdzone i by były w stanie zapewnić odpowiednią ochronę na właściwym poziomie bezpieczeństwa równoważnym poziomowi ochrony przyznawanemu na mocy przepisów bezpieczeństwa Rady Unii Europejskiej dotyczących ochrony informacji niejawnych UE, którym nadano odpowiadającą im klauzulę tajności, jak określono w umowie między państwami członkowskimi Unii Europejskiej, zebranymi w Radzie, w sprawie ochrony informacji niejawnych wymienianych w interesie Unii Europejskiej (2011/C 202/05) ([4]).

(3) Rada, Komisja i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa uzgodnili, że zapewnią maksymalną spójność w stosowaniu przepisów bezpieczeństwa dotyczących ochrony EUCI przez te instytucje, uwzględniając ich szczególne potrzeby instytucjonalne i organizacyjne, zgodnie z deklaracjami załączonymi do protokołu z posiedzenia Rady, na którym przyjęto decyzję Rady 2013/488/UE ([5]) w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE.

(4) Przepisy wykonawcze Komisji w zakresie bezpieczeństwa przemysłowego w odniesieniu do umów niejawnych powinny zatem zapewniać również maksymalny poziom spójności i uwzględniać wytyczne w sprawie bezpieczeństwa przemysłowego, zatwierdzone przez Komitet ds. Bezpieczeństwa Rady w dniu 13 grudnia 2016 r., i art. 7 i 22 dyrektywy Parlamentu Europejskiego i Rady 2009/81/WE ([6]).

(5) W dniu 4 maja 2016 r. Komisja przyjęła decyzję ([7]) upoważniającą członka Komisji odpowiedzialnego za kwestie bezpieczeństwa do przyjęcia w imieniu Komisji i na jej odpowiedzialność przepisów wykonawczych przewidzianych w art. 60 decyzji (UE, Euratom) 2015/444,

([1]) Dz.U. L 72 z 17.3.2015, s. 41.
([2]) Dz.U. L 72 z 17.3.2015, s. 53.
([3]) Dz.U. L 6 z 11.1.2017, s. 40.
([4]) Dz.U. C 202 z 8.7.2011, s. 13.
([5]) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).
([6]) Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z dnia 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa (Dz.U. L 216 z 20.8.2009, s. 76).
([7]) Decyzja Komisji z dnia 4 maja 2016 r. w sprawie upoważnienia związanego z bezpieczeństwem [C(2016) 2797 final].

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszej decyzji ustanawia się przepisy wykonawcze dotyczące bezpieczeństwa przemysłowego w odniesieniu do niejawnych zamówień publicznych w celu wsparcia wykonania decyzji (UE, Euratom) 2015/444, w szczególności jej rozdziału 6.

2. W niniejszej decyzji określono szczegółowe wymogi mające na celu zapewnienie ochrony informacji niejawnych UE (EUCI) przez podmioty gospodarcze na etapie poprzedzającym zawarcie umowy, na wszystkich etapach cyklu życia umów niejawnych zawartych przez Komisję Europejską oraz w umowach o podwykonawstwo zawieranych przez wykonawców Komisji.

3. Niniejsza decyzja dotyczy informacji niejawnych opatrzonych następującymi klauzulami tajności:

a) RESTREINT UE/EU RESTRICTED;

b) CONFIDENTIEL UE/EU CONFIDENTIAL;

c) SECRET UE/EU SECRET.

Artykuł 2

Zakres obowiązków wewnątrz Komisji

1. W ramach obowiązków opisanych w rozporządzeniu finansowym ([8]) każdy urzędnik zatwierdzający instytucji zamawiającej Komisji zapewnia, aby umowa niejawna odnosiła się do minimalnych standardów dotyczących bezpieczeństwa przemysłowego, określonych w rozdziale 6 decyzji (UE, Euratom) 2015/444 i w niniejszych przepisach wykonawczych oraz, w stosownych przypadkach, w ogłoszeniu o zamówieniu lub zaproszeniu do składania ofert, a także aby standardów tych przestrzegano w toku realizacji umowy.

2. W tym celu dany urzędnik zatwierdzający na wszystkich etapach korzysta z doradztwa organu ds. bezpieczeństwa Komisji w zakresie kwestii odnoszących się do elementów dotyczących bezpieczeństwa w umowie niejawnej, programie lub projekcie, a także informuje lokalnego pełnomocnika ochrony o zawartych umowach. Decyzję o poziomie klauzuli tajności nadawanym poszczególnym kwestiom podejmuje instytucja zamawiająca z należytym uwzględnieniem treści przewodnika nadawania klauzul.

3. W zakresie przestrzegania wymagań określonych w niniejszych przepisach wykonawczych organ ds. bezpieczeństwa Komisji prowadzi ścisłą współpracę z krajowymi władzami bezpieczeństwa (KWB) i wyznaczonymi władzami bezpieczeństwa (WWB) danego państwa członkowskiego, w szczególności w zakresie świadectw bezpieczeństwa przemysłowego (SBP) i poświadczeń bezpieczeństwa osobowego (PBO), procedur przeprowadzania wizyt i planów przewozu.

ROZDZIAŁ 2

POSTĘPOWANIE W PRZYPADKU ZAPROSZEŃ DO SKŁADANIA OFERT DOTYCZĄCYCH UMÓW NIEJAWNYCH

Artykuł 3

Podstawowe zasady

1. Umowy niejawne zawiera się wyłącznie z podmiotami gospodarczymi zarejestrowanymi w państwie członkowskim lub z podmiotami gospodarczymi zarejestrowanymi w państwie trzecim lub utworzonymi przez organizację międzynarodową, jeżeli takie państwo trzecie lub taka organizacja międzynarodowa zawarły umowę o bezpieczeństwie informacji z Unią Europejską lub porozumienie administracyjne z Komisją ([9]).

2. Przed ogłoszeniem zaproszenia do składania ofert dotyczącego umowy niejawnej instytucja zamawiająca określa klauzulę tajności wszelkich informacji, które mogą zostać udzielone oferentom. Instytucja zamawiająca określa również maksymalny poziom klauzuli tajności wszelkich informacji wygenerowanych w toku realizacji umowy, programu lub projektu, lub co najmniej przewidywaną ilość i rodzaj informacji, które zostaną wytworzone lub wykorzystane, a także konieczność stosowania systemu teleinformatycznego umożliwiającego korzystanie z informacji niejawnych.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

([9]) Na stronie internetowej Komisji można znaleźć wykaz umów zawartych przez UE i porozumień administracyjnych zawartych przez Komisję Europejską, na podstawie których można prowadzić wymianę informacji niejawnych UE z państwami trzecimi i organizacjami międzynarodowymi.

3. Instytucja zamawiająca zapewnia, aby ogłoszenia o zamówieniu dotyczące umów niejawnych zawierały informacje o szczególnych obowiązkach dotyczących bezpieczeństwa związanych z informacjami niejawnymi. Załącznik I zawiera przykładowy wzór informacji podawanych w ogłoszeniu o zamówieniu.

4. Instytucja zamawiająca zapewnia, aby informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET były ujawniane oferentom dopiero po podpisaniu przez nich umowy poufności zobowiązującej ich do korzystania z EUCI i ochrony takich informacji zgodnie z decyzją (UE, Euratom) 2015/444 i przepisami wykonawczymi do tej decyzji.

5. Wszyscy wykonawcy, którzy muszą korzystać z informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET lub przechowywać takie informacje w swoich obiektach już na etapie realizacji umowy niejawnej albo na etapie poprzedzającym zawarcie takiej umowy, posiadają świadectwo bezpieczeństwa przemysłowego na wymaganym poziomie. Poniżej przedstawiono trzy możliwe scenariusze na etapie procedury przetargowej dotyczącej umowy niejawnej obejmującej EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET:

a) brak dostępu do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET na etapie procedury przetargowej:

   jeżeli ogłoszenie o zamówieniu lub zaproszenie do składania ofert dotyczy umowy, która będzie obejmowała EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, ale oferent nie musi wykorzystywać takich informacji na etapie procedury przetargowej, wówczas z procedury przetargowej nie można wykluczyć oferenta, który nie posiada świadectwa bezpieczeństwa przemysłowego na wymaganym poziomie, ze względu na brak świadectwa bezpieczeństwa przemysłowego.

b) dostęp do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w obiektach instytucji zamawiającej na etapie procedury przetargowej:

   Dostęp zostaje udzielony pracownikom oferenta posiadającym PBO na wymaganym poziomie oraz zgodnie z zasadą ograniczonego dostępu. Zanim taki dostęp zostanie udzielony, instytucja zamawiająca sprawdza, konsultując się z odpowiednią KWB/WWB za pośrednictwem organu ds. bezpieczeństwa Komisji, czy na tym etapie świadectwo bezpieczeństwa przemysłowego jest wymagane również na podstawie krajowych przepisów ustawowych i wykonawczych;

c) korzystanie z EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET lub przechowywanie takich informacji w obiektach oferenta na etapie procedury przetargowej:

   jeżeli ogłoszenie o zamówieniu lub zaproszenie do składania ofert zawiera wymóg, zgodnie z którym oferenci muszą korzystać z EUCI lub przechowywać EUCI we własnych obiektach, wówczas oferent musi posiadać świadectwo bezpieczeństwa przemysłowego na wymaganym poziomie. W takiej sytuacji instytucja zamawiająca uzyskuje za pośrednictwem organu ds. bezpieczeństwa Komisji zaświadczenie od odpowiedniej KWB/WWB, że dany oferent uzyskał odpowiednie świadectwo bezpieczeństwa przemysłowego. Dostęp zostaje udzielony pracownikom oferenta posiadającym PBO na wymaganym poziomie oraz zgodnie z zasadą ograniczonego dostępu.

6. Zasadniczo posiadanie SBP do celów uzyskania dostępu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED nie jest wymagane ani na etapie procedury przetargowej, ani w toku wykonania umowy. Jeżeli na podstawie krajowych przepisów ustawowych i wykonawczych, wymienionych w załączniku IV, państwa członkowskie wymagają posiadania SBP w odniesieniu do umów lub umów o podwykonawstwo na poziomie RESTREINT UE/EU RESTRICTED, takie krajowe regulacje nie mogą nakładać żadnych dodatkowych obowiązków na pozostałe państwa członkowskie ani wykluczać oferentów, wykonawców lub podwykonawców z państw członkowskich, w których nie obowiązują takie wymogi dotyczące SBP w zakresie dostępu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, z wykonania powiązanych umów/umów o podwykonawstwo lub procedury dotyczącej takich umów. Takie umowy wykonuje się w państwach członkowskich zgodnie z ich krajowymi przepisami ustawowymi i wykonawczymi.

7. Jeżeli możliwość wykonania umowy niejawnej jest uzależniona od posiadania SBP, instytucja zamawiająca przedstawia za pośrednictwem organu ds. bezpieczeństwa Komisji wniosek do KWB/WWB wykonawcy, korzystając z arkusza informacyjnego dotyczącego SBP. Dodatek D do załącznika III zawiera przykładowy SBP ([10]). Zawarcie umowy niejawnej może nastąpić dopiero po potwierdzeniu SBP oferenta przez KWB/WWB wykonawcy. Odpowiedzi na przedstawiony arkusz informacyjny dotyczący SBP udziela się w miarę możliwości w terminie dziesięciu dni roboczych od daty złożenia wniosku.

([10]) Struktura innych formularzy znajdujących się w użyciu może różnić się od modelu przedstawionego w niniejszych przepisach wykonawczych.

Artykuł 4

Zawieranie umów o podwykonawstwo w przypadku umów niejawnych

1. Warunki zlecenia podwykonawstwa przez wykonawcę, z którym Komisja zawarła umowę niejawną, zostają określone w zaproszeniu do składania ofert i w dokumentach zamówienia. Jeżeli umowa niejawna dopuszcza realizację niektórych jej części w ramach podwykonawstwa, instytucja zamawiająca musi wcześniej wydać zgodę na takie podwykonawstwo. Przed wyrażeniem takiej zgody instytucja zamawiająca konsultuje się z organem ds. bezpieczeństwa Komisji.

2. W przypadku umów niejawnych podwykonawstwo zleca się wyłącznie podmiotom gospodarczym zarejestrowanym w państwie członkowskim lub podmiotom gospodarczym zarejestrowanym w państwie trzecim lub utworzonym przez organizację międzynarodową, jeżeli takie państwo trzecie lub taka organizacja międzynarodowa zawarły umowę o bezpieczeństwie informacji z UE lub porozumienie administracyjne z Komisją ([11]).

ROZDZIAŁ 3

ZAWIERANIE UMÓW NIEJAWNYCH PRZEZ KOMISJĘ

Artykuł 5

Podstawowe zasady

1. Przy zawieraniu umowy niejawnej instytucja zamawiająca wraz z organem ds. bezpieczeństwa Komisji zapewniają, aby obowiązki wykonawcy dotyczące ochrony EUCI przekazanych temu wykonawcy lub wygenerowanych w toku wykonywania umowy stanowiły integralną część umowy. Wymogi bezpieczeństwa dotyczące poszczególnych umów zawarte są w dokumencie określającym aspekty bezpieczeństwa (DOAB). Przykładowy wzór DOAB przedstawiono w załączniku III.

2. Przed podpisaniem umowy niejawnej instytucja zamawiająca sporządza po konsultacji z organem ds. bezpieczeństwa Komisji przewodnik nadawania klauzul (PNK) dotyczący przewidzianych do wykonania zadań i informacji generowanych w toku wykonania umowy lub w stosownych przypadkach na poziomie programu lub projektu. PKN stanowi część DOAB.

3. Wymogi bezpieczeństwa dotyczące poszczególnych programów lub projektów zawarte są w instrukcjach bezpieczeństwa programu lub projektu (IBP). IBP można opracować korzystając z przepisów zawartych we wzorze DOAB, jak określono w załączniku III. IBP opracowują służby Komisji zarządzające programem lub projektem, w ścisłej współpracy z organem ds. bezpieczeństwa Komisji, a następnie przedkładają je do zaopiniowania Grupie Ekspertów ds. Bezpieczeństwa Komisji. Jeżeli dana umowa stanowi część programu lub projektu objętego własnymi IBP, DOAB umowy ma formę uproszczoną i zawiera odesłanie do przepisów bezpieczeństwa określonych w IBP programu lub projektu.

4. Instytucję zamawiającą uznaje się za wytwórcę informacji niejawnych wytworzonych i wykorzystywanych w celu wykonania umowy.

5. Instytucja zamawiająca powiadamia za pośrednictwem organu ds. bezpieczeństwa Komisji KWB/WWB wszystkich wykonawców i podwykonawców o zawarciu umów niejawnych lub niejawnych umów o podwykonawstwo oraz o wszelkich przypadkach przedłużenia obowiązywania lub przedterminowego rozwiązania takich umów lub umów o podwykonawstwo. W załączniku IV znajduje się wykaz wymogów krajowych.

6. Umowy obejmujące informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED zawierają klauzulę umowną dotyczącą bezpieczeństwa, na mocy której przepisy określone w dodatku E do załącznika III są wiążące dla wykonawcy. Takie umowy zawierają DOAB, w którym określa się co najmniej wymogi dotyczące korzystania z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, w tym elementy potwierdzające informacje i szczególne wymogi, które musi spełnić wykonawca na podstawie przekazania kompetencji przez instytucję zamawiającą w celu uzyskania akredytacji CIS wykonawcy wykorzystującego informacje z klauzulą RESTREINT UE/EU RESTRICTED.

([11]) Na stronie internetowej Komisji można znaleźć wykaz umów zawartych przez UE i porozumień administracyjnych zawartych przez Komisję Europejską, na podstawie których można prowadzić wymianę informacji niejawnych UE z państwami trzecimi i organizacjami międzynarodowymi.

7. Jeżeli informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED zostają udzielone oferentom lub potencjalnym wykonawcom, minimalne wymogi, o których mowa w ust. 6, zostają uwzględnione w ofercie lub w odpowiedniej umowie o zachowaniu poufności zawartej na koniec procedury przetargowej.

8. Jeżeli wymagają tego krajowe przepisy ustawowe i wykonawcze państw członkowskich, KWB/WWB zapewniają, aby podlegający ich jurysdykcji wykonawcy lub podwykonawcy przestrzegali obowiązujących przepisów bezpieczeństwa dotyczących ochrony informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, a także przeprowadzają wizyty weryfikacyjne w obiektach wykonawców znajdujących się na podlegającym im terytorium. Jeżeli KWB/WWB nie ma takiego obowiązku, instytucja zamawiająca zapewnia, aby wykonawca przestrzegał przepisów dotyczących wymaganego poziomu bezpieczeństwa, określonych w załączniku III.

Artykuł 6

Dostęp pracowników wykonawców i podwykonawców do EUCI

1. Departament Komisji, jako instytucja zamawiająca, zapewnia, aby umowy niejawne zawierały postanowienia wskazujące, że pracownicy wykonawcy lub podwykonawcy, którzy do wykonania umowy niejawnej lub niejawnej umowy o podwykonawstwo potrzebują dostępu do EUCI, mogą uzyskać taki dostęp, pod warunkiem że:

a) ustalono, że potrzebują takiego dostępu na zasadzie ograniczonego dostępu;

b) otrzymali od KWB/WWB lub jakiegokolwiek innego właściwego organu ds. bezpieczeństwa PBO do odpowiedniego poziomu informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET;

c) zostali poinformowani o obowiązujących przepisach bezpieczeństwa służących ochronie EUCI i potwierdzili, że zapoznali się ze swoimi obowiązkami w zakresie ochrony takich informacji.

2. Jeżeli wykonawca lub podwykonawca zamierza zatrudnić obywatela państwa trzeciego na stanowisku wymagającym dostępu do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, zadaniem wykonawcy lub podwykonawcy jest wszczęcie procedury sprawdzającej w zakresie poświadczenia bezpieczeństwa wobec takiej osoby zgodnie z krajowymi przepisami ustawowymi i wykonawczymi obowiązującymi w miejscu, w którym ma zostać udzielony dostęp do EUCI.

ROZDZIAŁ 4

WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI

Artykuł 7

Podstawowe zasady

1. Jeżeli Komisji, wykonawcom lub podwykonawcom niezbędny jest w związku z wykonaniem umowy niejawnej dostęp do informacji niejawnych z klauzulą 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.

2. Wizyty, o których mowa w ust. 1, podlegają następującym wymogom:

a) wizyta przeprowadzana jest w celach oficjalnych związanych z umową niejawną zawartą przez Komisję;

b) każda osoba wizytująca posiada PBO na wymaganym poziomie i kieruje się zasadą ograniczonego dostępu do EUCI udzielanych lub generowanych w toku wykonania umowy niejawnej zawartej przez Komisję.

Artykuł 8

Wnioski o wizyty

1. Wizyty wykonawców w obiektach innych wykonawców lub Komisji, które obejmują dostęp do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET organizuje się zgodnie z następującą procedurą:

a) pełnomocnik ochrony obiektu wysyłający osobę wizytującą wypełnia wszystkie stosowne części wniosku o wizytę i składa wniosek do KWB/WWB właściwej dla danego obiektu. Wzór formularza wniosku o wizytę przedstawiono w dodatku C do załącznika III;

b) KWB/WWB właściwa dla obiektu wysyłającego musi potwierdzić PBO osoby wizytującej przed złożeniem wniosku o wizytę do KWB/WWB właściwej dla wizytowanego obiektu (lub do organu ds. bezpieczeństwa Komisji, jeżeli wizyta ma przebiegać w obiektach należących do Komisji);

c) pełnomocnik ochrony obiektu wysyłającego otrzymuje wtedy od swojej KWB/WWB odpowiedź KWB/WWB właściwej dla wizytowanego obiektu (lub organu ds. bezpieczeństwa Komisji) zatwierdzającą albo odrzucającą wniosek o wizytę;

d) wniosek o wizytę uznaje się za zatwierdzony, jeżeli w terminie do pięciu dni roboczych przed datą wizyty nie zostaną zgłoszone żadne zastrzeżenia.

2. Wizyty urzędników Komisji w obiektach wykonawcy, które obejmują dostęp do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, organizuje się zgodnie z następującą procedurą:

a) osoba wizytująca wypełnia wszystkie stosowne części wniosku o wizytę i składa wniosek do organu ds. bezpieczeństwa Komisji;

b) organ ds. bezpieczeństwa Komisji potwierdza PBO osoby wizytującej przed złożeniem wniosku o wizytę do KWB/WWB właściwej dla wizytowanego obiektu;

c) organ ds. bezpieczeństwa Komisji uzyskuje odpowiedź KWB/WWB wizytowanego obiektu zatwierdzającą albo odrzucającą wniosek o wizytę;

d) wniosek o wizytę uznaje się za zatwierdzony, jeżeli w terminie do pięciu dni roboczych przed datą wizyty nie zostaną zgłoszone żadne zastrzeżenia.

3. Wniosek o wizytę może dotyczyć pojedynczej wizyty albo powtarzających się wizyt. W przypadku powtarzających się wizyt wniosek o wizytę może obowiązywać maksymalnie przez rok od daty początkowej określonej we wniosku.

4. Okres ważności wniosku o wizytę nie może przekraczać okresu ważności PBO osoby wizytującej.

5. Zasadniczo wniosek o wizytę należy przedstawiać właściwemu organowi bezpieczeństwa, któremu podlega wizytowany obiekt, w terminie co najmniej 15 dni roboczych przed datą wizyty.

Artykuł 9

Procedury przeprowadzania wizyt

1. Przed umożliwieniem osobie wizytującej dostępu do EUCI pełnomocnik ochrony wizytowanego obiektu stosuje wszystkie procedury bezpieczeństwa i wszystkie zasady związane z wizytą określone przez właściwą KWB/WWB.

2. Osoby wizytujące potwierdzają swoją tożsamość po przybyciu do wizytowanego obiektu, okazując ważny dokument tożsamości lub paszport. Takie informacje potwierdzające tożsamość muszą odpowiadać informacjom przedstawionym we wniosku o wizytę.

3. Wizytowany obiekt zapewnia przechowywanie rejestrów z danymi dotyczącymi wszystkich osób wizytujących, m.in. ich imion i nazwisk, nazwy reprezentowanej organizacji, daty wygaśnięcia PBO, daty wizyty oraz imion i nazwisk osób, u których przeprowadzana jest wizyta. Takie dane przechowuje się przez okres co najmniej pięciu lat lub, w razie potrzeby, przez dłuższy okres, jeżeli stanowią tak krajowe zasady i przepisy w państwie, na terenie którego znajduje się wizytowany obiekt.

Artykuł 10

Wizyty organizowane bezpośrednio

1. W kontekście konkretnych projektów właściwe KWB/WWB i organ ds. bezpieczeństwa Komisji mogą uzgodnić procedurę, zgodnie z którą pełnomocnik ochrony osoby wizytującej i pełnomocnik ochrony wizytowanego obiektu mogą bezpośrednio organizować wizyty dotyczące konkretnej umowy niejawnej. Wzór przeznaczonego do stosowania w tym celu formularza przedstawiono w dodatku C do załącznika III. Taka szczególna procedura zostaje określona w IBP lub w ramach innego rodzaju szczególnych ustaleń. W takich przypadkach nie mają zastosowania procedury określone w art. 8 i art. 9 ust. 1.

2. Wizyty obejmujące dostęp do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED są organizowane bezpośrednio między podmiotami wysyłającymi i wizytowanymi bez konieczności przestrzegania procedury opisanej w art. 8 i art. 9 ust. 1.

ROZDZIAŁ 5

TRANSMISJA I PRZEMIESZCZANIE EUCI W TOKU WYKONANIA UMÓW NIEJAWNYCH

Artykuł 11

Podstawowe zasady

Instytucja zamawiająca zapewnia, aby wszystkie decyzje związane z przekazywaniem i przemieszczaniem EUCI były zgodne z decyzją (UE, Euratom) 2015/444 i przepisami wykonawczymi do tej decyzji oraz z warunkami umowy niejawnej, w tym z uwzględnieniem zgody wytwórcy.

Artykuł 12

Elektroniczne wykorzystywanie

1. Elektroniczne wykorzystywanie i przekazywanie EUCI odbywa się zgodnie z rozdziałami 5 i 6 decyzji (UE, Euratom) 2015/444 i przepisami wykonawczymi do tej decyzji.

Systemy teleinformatyczne będące własnością wykonawcy i używane przy wykorzystywaniu EUCI w toku wykonania umowy (zwane dalej „CIS wykonawcy") podlegają akredytacji przez odpowiedzialny organ ds. akredytacji bezpieczeństwa (SAA). Wszelkie elektroniczne przekazywanie EUCI podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 36 ust. 4 decyzji (UE, Euratom) 2015/444. Środki TEMPEST są wdrażanie zgodnie z art. 36 ust. 6 tej decyzji.

2. Akredytację bezpieczeństwa CIS wykonawcy obsługującego EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED oraz jakichkolwiek jego połączeń międzysystemowych można zlecić pełnomocnikowi ochrony wykonawcy, jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość. Jeżeli zadanie to zostaje oddelegowane, wykonawca odpowiada za wdrożenie minimalnych wymogów bezpieczeństwa opisanych w DOAB przy korzystaniu z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED za pomocą CIS. Odpowiednie KWB/WWB/SAA pozostają jednak odpowiedzialne za ochronę informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, z których korzysta wykonawca, a także zachowują prawo do kontroli środków bezpieczeństwa wprowadzonych przez wykonawcę. Ponadto wykonawca przekazuje instytucji zamawiającej i, jeżeli jest to wymagane w krajowych przepisach ustawowych i wykonawczych, właściwemu krajowemu SAA stwierdzenie o zgodności poświadczające, że CIS wykonawcy i jego połączenia międzysystemowe otrzymały akredytację do przetwarzania EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED ([12]).

Artykuł 13

Transport przez kurierów komercyjnych

Transport EUCI przez kurierów komercyjnych musi być zgodny z odpowiednimi przepisami decyzji Komisji w sprawie przepisów wykonawczych dotyczących korzystania z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED i z informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL.

Artykuł 14

Przenoszenie osobiste

1. Osobiste przenoszenie informacji niejawnych podlega rygorystycznym wymogom bezpieczeństwa.

2. Pracownicy wykonawcy w UE mogą osobiście przenosić informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED, pod warunkiem że spełnione są następujące wymogi:

a) zastosowano nieprzezroczyste opakowanie lub kopertę bez żadnych oznaczeń wskazujących, że w środku znajdują się informacje niejawne;

([12]) Minimalne wymogi dotyczące systemów teleinformatycznych, w których korzysta się z EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED, określono w dodatku E do załącznika III.

b) informacje niejawne przez cały czas znajdują się w posiadaniu osoby je przenoszącej;

c) koperta lub opakowanie nie są po drodze otwierane.

3. Warunki osobistego przenoszenia informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET przez pracowników wykonawcy na terenie państw członkowskich UE są ustalane z wyprzedzeniem przez podmiot wysyłający i otrzymujący. Organ lub obiekt przesyłający przekazuje organowi lub obiektowi otrzymującemu informacje na temat przesyłki, w tym numer referencyjny, poziom klauzuli tajności, oczekiwany czas otrzymania i imię i nazwisko kuriera. Tego rodzaju osobiste przenoszenie jest dozwolone, pod warunkiem że spełnione są następujące wymogi:

a) informacje niejawne przenoszone są w dwóch kopertach lub opakowaniach;

b) zewnętrzne opakowanie lub koperta są zabezpieczone i nie zawierają żadnych oznaczeń wskazujących na poziom klauzuli tajności zawartości, który wskazano natomiast na wewnętrznej kopercie;

c) EUCI przez cały czas znajdują się w posiadaniu osoby je przenoszącej;

d) koperta lub opakowanie nie są po drodze otwierane;

e) koperta lub opakowanie są przenoszone w aktówce wyposażonej w zamek lub w podobnym zatwierdzonym pojemniku o takim kształcie i masie, że może się on przez cały czas znajdować się w posiadaniu osoby go przewożącej bez umieszczania w luku bagażowym;

f) kurier ma przy sobie list kurierski wydany przez właściwy organ bezpieczeństwa, któremu podlega, upoważniający kuriera do przewozu wskazanej przesyłki niejawnej.

4. W przypadku osobistego przenoszenia informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET przez pracowników wykonawcy między państwami członkowskimi UE zastosowanie mają następujące przepisy dodatkowe:

a) kurier odpowiada za bezpieczne przechowanie materiałów niejawnych do momentu ich przekazania odbiorcy;

b) w przypadku naruszenia bezpieczeństwa KWB/WWB właściwa dla nadawcy może żądać od organów państwa, w którym doszło do naruszenia bezpieczeństwa, przeprowadzenia dochodzenia, przedstawienia ustaleń z takiego dochodzenia oraz w stosownych przypadkach wszczęcia postępowania sądowego lub podjęcia innych działań;

c) przed przejęciem przesyłki kurier został powiadomiony o wszystkich obowiązkach dotyczących bezpieczeństwa, których należy przestrzegać podczas przemieszczania informacji, i podpisał stosowne oświadczenia;

d) do listu kurierskiego załączona zostaje instrukcja przeznaczona dla kuriera;

e) kurier otrzymał wcześniej opis przesyłki i trasy;

f) dokumenty zostają zwrócone wydającej je KWB/WWB po zakończeniu podróży lub odbiorca przechowuje je i udostępnia do celów monitorowania;

g) jeżeli organy celne, imigracyjne lub policja graniczna zażądają okazania przesyłki do kontroli, dopuszcza się otwarcie i zobaczenie przez takie organy części przesyłki wystarczających do stwierdzenia, że zawiera ona wyłącznie zadeklarowane materiały;

h) organy celne należy wezwać do uhonorowania faktu wystawienia przez władzę publiczną dokumentów przewozowych i dokumentów uwierzytelniających posiadanych przez kuriera.

Jeżeli organy celne otwierają przesyłkę, musi to odbywać się poza zasięgiem wzroku osób nieupoważnionych i w miarę możliwości w obecności kuriera. Kurier musi poprosić o ponowne zapakowanie przesyłki i zażądać od organów przeprowadzających kontrolę ponownego zapieczętowania przesyłki i pisemnego potwierdzenia, że przesyłka została otarta przez te organy.

5. Osobiste przenoszenie przez pracowników wykonawcy informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET na terytorium państwa trzeciego lub do organizacji międzynarodowej będzie podlegało postanowieniom umowy o bezpieczeństwie informacji lub porozumienia administracyjnego zawartych odpowiednio między Unią Europejską albo Komisją a takim państwem trzecim albo taką organizacją międzynarodową.

ROZDZIAŁ 6

PLANOWANIE CIĄGŁOŚCI DZIAŁANIA

Artykuł 15

Plany awaryjne i środki naprawcze

Departament Komisji, jako instytucja zamawiająca, zapewnia, aby umowa niejawna zawierała wymóg, zgodnie z którym wykonawca musi opracować firmowe plany awaryjne w celu ochrony wszelkich EUCI wykorzystywanych w związku z wykonywaniem umowy niejawnej w sytuacjach awaryjnych i wprowadzić środki zapobiegawcze i naprawcze w kontekście planowania ciągłości działania służące zminimalizowaniu skutków incydentów związanych z wykorzystywaniem EUCI oraz z ich przechowywaniem. Wykonawca lub podwykonawca informuje instytucję zamawiającą o swoich planach awaryjnych.

Artykuł 16

Wejście w życie

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

Sporządzono w Brukseli dnia 17 października 2019 r.

W imieniu Komisji,

za Przewodniczącego,

Günther OETTINGER

Członek Komisji

ZAŁĄCZNIK I

STANDARDOWE INFORMACJE W OGŁOSZENIACH O ZAMÓWIENIU PUBLICZNYM

(które mają być dostosowane do wykorzystywanych ogłoszeń o zamówieniu)

W przypadku umów obejmujących informacje niejawne z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET

Inne szczególne warunki (*w stosownych przypadkach*)

Wykonanie umowy podlega szczególnym warunkom ● tak ○ nie

(*jeżeli tak*) Opis szczególnych warunków:

Taka umowa obejmować będzie udostępnienie, wykorzystywanie lub przechowywanie informacji niejawnych z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, które podlegają przepisom bezpieczeństwa dotyczącym ochrony informacji niejawnych UE określonym w decyzji (UE, Euratom) 2015/444 i jej przepisach wykonawczych ([1]).

Wymagane będzie świadectwo bezpieczeństwa przemysłowego, jak również poświadczenie bezpieczeństwa osobowego w odniesieniu do pracowników wykonawcy, którzy wykorzystują informacje niejawne.

W skład umowy wchodzić będą szczególne obowiązki w zakresie bezpieczeństwa (dokument określający aspekty bezpieczeństwa załączony do umowy). Podwykonawstwo wymagać będzie uprzedniego uzyskania pisemnej zgody od instytucji zamawiającej oraz przestrzegania wszystkich przepisów bezpieczeństwa przez podwykonawcę i jego pracowników.

W przypadku umów obejmujących informacje niejawne z klauzulą tajności RESTREINT UE/EU RESTRICTED

Inne szczególne warunki (*w stosownych przypadkach*)

Wykonanie umowy podlega szczególnym warunkom ● tak ○ nie

(*jeżeli tak*) Opis szczególnych warunków:

Umowa będzie obejmować udostępnienie, wykorzystywanie lub przechowywanie lub skutkować udostępnieniem, wykorzystywaniem lub przechowywaniem informacji niejawnych z klauzulą tajności RESTREINT UE/EU RESTRICTED, które podlegają przepisom bezpieczeństwa dotyczącym ochrony informacji niejawnych UE określonym w decyzji (UE, Euratom) 2015/444 i jej przepisach wykonawczych ([2]).

W skład umowy wchodzić będą szczególne obowiązki w zakresie bezpieczeństwa (dokument określający aspekty bezpieczeństwa załączony do umowy). Podwykonawstwo wymagać będzie uprzedniego uzyskania pisemnej zgody od instytucji zamawiającej oraz przestrzegania wszystkich przepisów bezpieczeństwa przez podwykonawcę i jego pracowników.

([1]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.
([2]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.

ZAŁĄCZNIK II

STANDARDOWE KLAUZULE UMOWNE W ZAMÓWIENIACH PUBLICZNYCH

(do dostosowania do stosowanych umów)

ARTYKUŁ XX

OBOWIĄZKI ZWIĄZANE Z BEZPIECZEŃSTWEM

XX.1 Informacje niejawne UE

Jeżeli realizacja umowy obejmuje wykorzystywanie lub tworzenie informacji niejawnych UE, informacje takie muszą być traktowane zgodnie z dokumentem określającym aspekty bezpieczeństwa (DOAB) i stanowiącym jego część przewodnikiem nadawania klauzul (PNK), jak określono w Załączniku 1, oraz z decyzją (UE, Euratom) 2015/444 i jej przepisami wykonawczymi [1], do momentu, aż klauzula tajności zostanie zniesiona.

Wszelkie dokumenty zawierające informacje niejawne należy składać przestrzegając specjalnych procedur ustalonych z instytucją zamawiającą.

Nie można zlecać podwykonawstwa żadnych zadań wiążących się z informacjami niejawnymi bez uprzedniego uzyskania wyraźnej pisemnej zgody instytucji zamawiającej.

Informacji niejawnych UE nie można ujawniać żadnej osobie trzeciej (w tym podwykonawcom) bez uprzedniego uzyskania wyraźnej pisemnej zgody instytucji zamawiającej.

[1] Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.

ZAŁĄCZNIK III

[Załącznik IV (do Umowy Ramowej)]

DOKUMENT OKREŚLAJĄCY ASPEKTY BEZPIECZEŃSTWA (DOAB)

[Wzór]

Dodatek A

WYMOGI W ZAKRESIE BEZPIECZEŃSTWA

Instytucja zamawiająca musi włączyć do dokumentu określającego aspekty bezpieczeństwa (DOAB) następujące wymagania w zakresie bezpieczeństwa. Niektóre klauzule mogą nie mieć zastosowania do umowy. Zostały one ujęte w kwadratowe nawiasy.

Lista klauzul nie jest wyczerpująca. Dalsze klauzule mogą zostać dodane w zależności od charakteru umowy niejawnej.

WARUNKI OGÓLNE

[*N.B.: mają zastosowanie do wszystkich umów niejawnych*]

1. W niniejszym dokumencie określającym aspekty bezpieczeństwa (DOAB), stanowiącym integralną część umowy niejawnej [lub umowy niejawnej o podwykonawstwo], opisano wymagania w zakresie bezpieczeństwa odnoszące się do konkretnej umowy. Niespełnienie tych wymagań może stanowić wystarczającą podstawę do rozwiązania umowy.

2. Wykonawcy podlegają wszystkim obowiązkom określonym w decyzji (UE, Euratom) 2015/444 oraz w jej przepisach wykonawczych ([1]).

3. Informacje niejawne wytworzone podczas wykonywania umowy muszą zostać oznaczone jako informacje niejawne UE (EUCI) na poziomie klauzuli tajności, jak określono w przewodniku nadawania klauzul (PNK) w Dodatku B do niniejszego dokumentu. Odstępstwo od poziomu klauzuli tajności określonego w PNK jest dopuszczalne wyłącznie pod warunkiem uzyskania pisemnego pozwolenia instytucji zamawiającej.

4. Prawa dotyczące wytwórcy wszelkich EUCI wytworzonych i wykorzystywanych w celu wykonania umowy niejawnej wykonuje Komisja jako instytucja zamawiająca.

5. Bez pisemnej zgody instytucji zamawiającej wykonawca lub podwykonawca nie może wykorzystywać żadnych informacji ani materiałów dostarczonych przez instytucję zamawiającą lub wytworzonych w jej imieniu w żadnym innym celu niż cel, jaki ma umowa.

6. Wykonawca ma obowiązek badać wszelkie przypadki naruszenia bezpieczeństwa związane z EUCI i możliwie jak najszybciej zgłaszać je instytucji zamawiającej. Wykonawca lub podwykonawca niezwłocznie zgłasza odpowiedzialnej krajowej władzy bezpieczeństwa (KWB) lub wyznaczonej władzy bezpieczeństwa (WWB) oraz, w przypadku gdy jest to dozwolone na podstawie krajowych przepisów ustawowych i wykonawczych, organowi ds. bezpieczeństwa Komisji, wszystkie przypadki, co do których wiadomo, lub co do których istnieją powody, by podejrzewać, że EUCI dostarczone lub wytworzone zgodnie z umową zostały utracone lub ujawnione osobom nieupoważnionym.

7. Po zakończeniu obowiązywania umowy wykonawca lub podwykonawca ma obowiązek jak najszybciej zwrócić instytucji zamawiającej wszelkie posiadane EUCI. Jeżeli jest to wykonalne, wykonawca lub podwykonawca może zniszczyć EUCI, zamiast je zwracać. Należy to zrobić zgodnie z przepisami ustawowymi i wykonawczymi kraju, w którym wykonawca ma siedzibę, po uzyskaniu uprzedniej zgody organu ds. bezpieczeństwa Komisji i według jego instrukcji. EUCI muszą zostać zniszczone w taki sposób, by nie mogły zostać całkowicie lub częściowo odtworzone.

8. W przypadku, gdy wykonawca lub podwykonawca jest upoważniony do zachowania EUCI po zakończeniu obowiązywania umowy lub jej rozwiązaniu, EUCI muszą nadal podlegać ochronie zgodnie z decyzją (UE, Euratom) 2015/444 (zwaną dalej „DK 2015/444"), a także jej przepisami wykonawczymi ([2]).

9. Elektroniczne wykorzystywanie, przetwarzanie i przekazywanie EUCI musi odbywać się zgodnie z przepisami określonymi w Rozdziale 5 i 6 DK 2015/444. Obejmują one między innymi wymóg, by systemy teleinformatyczne będące własnością wykonawcy i używane do celów wykorzystywania EUCI na potrzeby realizacji umowy (zwane dalej „CIS wykonawcy") podlegały akredytacji ([3]); by każda transmisja elektroniczna EUCI była chroniona za pomocą produktów kryptograficznych zatwierdzonych zgodnie z art. 36 ust. 4 DK 2015/444 oraz by środki TEMPEST były wdrożone zgodnie z art. 36 ust. 6 DK 2015/444.

([1]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.
([2]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.
([3]) Strona przeprowadzająca akredytację będzie musiała dostarczyć instytucji zamawiającej stwierdzenie zgodności za pośrednictwem organu ds. bezpieczeństwa Komisji oraz we współpracy ze stosownym krajowym organem ds. akredytacji bezpieczeństwa (SAA).

10. Wykonawca lub podwykonawca posiada firmowe plany awaryjne w celu ochrony wszelkich EUCI wykorzystywanych podczas wykonywania umowy niejawnej w sytuacjach awaryjnych oraz wprowadza środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków incydentów związanych z wykorzystywaniem EUCI oraz z ich przechowywaniem. Wykonawca lub podwykonawca musi poinformować instytucję zamawiającą o swoich planach awaryjnych.

UMOWY WYMAGAJĄCE DOSTĘPU DO INFORMACJI Z KLAUZULĄ TAJNOŚCI RESTREINT UE/EU RESTRICTED

11. Poświadczenie bezpieczeństwa osobowego (PBO) nie jest wymagane dla zachowania zgodności z umową. Informacje lub materiały z klauzulą tajności RESTREINT UE/EU RESTRICTED mogą być jednak dostępne wyłącznie dla pracowników wykonawcy, którzy potrzebują tych informacji w celu wykonania umowy (*zasada ograniczonego dostępu*), zostali poinformowani przez pełnomocnika ochrony wykonawcy o swoich obowiązkach i o konsekwencjach naruszenia bezpieczeństwa tych informacji oraz narażenia ich na szwank, i którzy zaakceptowali na piśmie konsekwencje niezapewniania ochrony EUCI.

12. Z wyjątkiem przypadku, w którym instytucja zamawiająca wyraziła pisemną zgodę, wykonawca lub podwykonawca nie może udostępniać informacji lub materiałów z klauzulą tajności RESTREINT UE/EU RESTRICTED żadnemu podmiotowi ani osobie, poza pracownikami objętymi zasadą ograniczonego dostępu.

13. Wykonawca lub podwykonawca musi zachować oznaczenia klauzuli tajności informacji niejawnych wytworzonych lub dostarczonych podczas wykonywania umowy i nie może znieść klauzul tajności informacji bez uzyskania pisemnej zgody instytucji zamawiającej.

14. Informacje lub materiały z klauzulą tajności RESTREINT UE/EU RESTRICTED muszą być przechowywane w zamkniętym meblu biurowym, gdy nie są wykorzystywane. Przekazywane dokumenty muszą być umieszczone w nieprzezroczystej kopercie. Dokumenty muszą przez cały czas znajdować się w posiadaniu osoby sprawującej nad nimi pieczę i nie mogą być po drodze otwierane.

15. Wykonawca lub podwykonawca może przekazać Komisji dokumenty z klauzulą tajności RESTREINT UE/EU RESTRICTED korzystając z usług komercyjnych przedsiębiorstw kurierskich, za pośrednictwem usług pocztowych, osobiście lub drogą elektroniczną. W tym celu wykonawca lub podwykonawca musi postępować zgodnie z instrukcją bezpieczeństwa programu (lub projektu) (IBP) wydaną przez Komisję lub z przepisami wykonawczymi Komisji dotyczącymi bezpieczeństwa przemysłowego w odniesieniu do niejawnych umów w sprawie zamówienia publicznego ([4]).

16. Kiedy dokumenty z klauzulą tajności RESTREINT UE/EU RESTRICTED przestają już być potrzebne, należy je zniszczyć w taki sposób, by nie mogły zostać całkowicie lub częściowo odtworzone.

17. Akredytację bezpieczeństwa CIS wykonawcy wykorzystującego EUCI na poziomie RESTREINT UE/EU RESTRICTED oraz jakiekolwiek połączenia międzysystemowe można zlecić pełnomocnikowi ochrony wykonawcy, jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość. W przypadku gdy akredytacja zostaje w taki sposób zlecona, KWB/WWB/SAA pozostają odpowiedzialne za ochronę wszelkich informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED wykorzystywanych przez wykonawcę i zachowują prawo do kontroli środków bezpieczeństwa wprowadzonych przez wykonawcę. Ponadto wykonawca przekazuje instytucji zamawiającej, a jeżeli jest to wymagane zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, właściwemu krajowemu SAA stwierdzenie o zgodności poświadczające, że CIS wykonawcy i związane z nim połączenia międzysystemowe otrzymały akredytację do korzystania z EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED.

WYKORZYSTYWANIE INFORMACJI Z KLAUZULĄ TAJNOŚCI RESTREINT UE/EU RESTRICTED W SYSTEMACH TELEINFORMATYCZNYCH (CIS)

18. Wymagania minimalne dla CIS, w których wykorzystuje się informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED przedstawiono w dodatku E do DOAB.

WARUNKI, NA KTÓRYCH WYKONAWCA MOŻE ZLECIĆ PODWYKONAWSTWO

19. Wykonawca musi uzyskać zgodę właściwego departamentu Komisji jako instytucji zamawiającej zanim zleci podwykonawstwo jakiejkolwiek części umowy niejawnej.

([4]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.

20. Nie można zlecać podwykonawstwa przedsiębiorstwu zarejestrowanemu w państwie niebędącym członkiem UE ani podmiotowi należącemu do organizacji międzynarodowej, jeżeli to państwo niebędące członkiem UE lub ta organizacja międzynarodowa nie zawarły umowy o bezpieczeństwie informacji z UE lub umowy administracyjnej z Komisją.

21. W przypadku gdy wykonawca zlecił podwykonawstwo, przepisy bezpieczeństwa stosuje się odpowiednio do podwykonawcy (podwykonawców) i jego (ich) pracowników. W takiej sytuacji na wykonawcy spoczywa odpowiedzialność za zapewnienie, aby wszyscy podwykonawcy stosowali te zasady w swoich własnych umowach o podwykonawstwo. Aby zapewnić odpowiednią kontrolę bezpieczeństwa, należy powiadomić KWB/WWB wykonawcy i podwykonawcy o wszelkich powiązanych niejawnych umowach o podwykonawstwo z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET. W stosownych przypadkach należy przekazać KWB/WWB wykonawcy i podwykonawcy egzemplarz przepisów bezpieczeństwa dotyczących umowy o podwykonawstwo. KWB/WWB wymagające powiadomienia o przepisach bezpieczeństwa zawartych w umowach niejawnych z klauzulą tajności RESTREINT UE/EU RESTRICTED wymieniono w załączniku do przepisów wykonawczych Komisji dotyczących bezpieczeństwa przemysłowego odnoszących się do niejawnych zamówień publicznych ([1]).

22. Wykonawca nie może przekazać żadnych EUCI podwykonawcy bez uprzedniej zgody instytucji zamawiającej. Jeżeli EUCI mają być przekazywane często lub regularnie, wtedy instytucja zamawiająca może wyrazić zgodę na określony okres (np. 12 miesięcy) lub na czas trwania umowy o podwykonawstwo.

WIZYTY

Jeżeli standardowa procedura wniosku o wizytę (RFV) ma być stosowana do wizyt obejmujących informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, wtedy instytucja zamawiająca musi uwzględnić pkt 23, 24 i 25 i usunąć pkt 26. W przypadku gdy wizyty dotyczące informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET są organizowane bezpośrednio między instytucjami wysyłającymi i przyjmującymi, instytucja zamawiająca musi usunąć pkt 24 i 25, a uwzględnić jedynie pkt 26.

23. Wizyty dotyczące dostępu lub potencjalnego dostępu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED są organizowane bezpośrednio między instytucjami wysyłającymi i przyjmującymi, bez konieczności przestrzegania procedury opisanej w pkt 24–26 poniżej.

[24. Wizyty dotyczące dostępu lub potencjalnego dostępu do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET podlegają następującej procedurze:

a) pełnomocnik ochrony obiektu wysyłającego osobę wizytującą wypełnia wszystkie odpowiednie części wniosku o wizytę (dodatek C) i składa wniosek do KWB/WWB właściwej dla danego obiektu;

b) KWB/WWB obiektu wysyłającego musi potwierdzić PBO osoby wizytującej przed złożeniem wniosku o wizytę do KWB/WWB wizytowanego obiektu (lub do organu ds. bezpieczeństwa Komisji, jeżeli wizyta ma przebiegać w siedzibie Komisji);

c) pełnomocnik ochrony obiektu wysyłającego uzyskuje wtedy od swojej KWB/WWB odpowiedź KWB/WWB wizytowanego obiektu (lub organu ds. bezpieczeństwa Komisji) zawierającą zatwierdzenie wniosku o wizytę albo jego odrzucenie;

d) wniosek o wizytę uznaje się za zatwierdzony, jeżeli w terminie do pięciu dni roboczych przed datą wizyty nie zostanie zgłoszony żaden sprzeciw.]

[25. Przed udzieleniem osobie wizytującej (osobom wizytującym) dostępu do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET wizytowany obiekt musi otrzymać zgodę swojej KWB/WWB.]

[26. Wizyty dotyczące dostępu lub potencjalnego dostępu do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET są organizowane bezpośrednio między instytucjami wysyłającymi i wizytowanymi (przykład formularza, który można wykorzystać w tym celu, zamieszczono w dodatku C).]

([1]) Instytucja zamawiająca musi w umowie zamieścić odniesienia po przyjęciu przepisów wykonawczych.

27. Osoby wizytujące muszą potwierdzić swoją tożsamość po przybyciu do wizytowanego obiektu, okazując ważny dokument tożsamości lub paszport.

28. Obiekt, w którym odbywa się wizyta, musi zapewnić przechowywanie danych wszystkich osób wizytujących. Muszą one obejmować imiona i nazwiska, nazwę reprezentowanej organizacji, datę wygaśnięcia PBO (w stosownych przypadkach), datę wizyty oraz imię i nazwisko odwiedzanej osoby. Takie dane przechowuje się, bez uszczerbku dla europejskich przepisów w zakresie ochrony danych, przez okres co najmniej pięciu lat lub, w stosownych przypadkach, zgodnie z przepisami krajowymi.

WIZYTY OCENIAJĄCE

29. Organ ds. bezpieczeństwa Komisji może we współpracy z właściwą KWB/WWB przeprowadzić wizyty w obiektach wykonawcy lub podwykonawcy, aby sprawdzić, czy przestrzegane są wymagania bezpieczeństwa w zakresie przetwarzania EUCI.

PRZEWODNIK NADAWANIA KLAUZUL

30. Przewodnik nadawania klauzul (PNK) obejmuje wykaz wszystkich elementów umowy, które są niejawne lub takie się staną w toku wykonywania umowy, zasady przeprowadzania utajniania i mające zastosowanie poziomy klauzuli tajności. PNK stanowi integralną część tej umowy i znajduje się w dodatku B do niniejszego załącznika.

Dodatek B

PRZEWODNIK NADAWANIA KLAUZUL

[konkretny tekst dopasowuje się w zależności od przedmiotu umowy]

Dodatek C

WNIOSEK O WIZYTĘ

(MODEL)

Dokładna instrukcja wypełniania wniosku o wizytę

(Wniosek należy złożyć w języku angielskim)

HEADING	Należy zaznaczyć pole wyboru dotyczące rodzaju wizyty, rodzaju informacji oraz wskazać liczbę wizytowanych miejsc i liczbę osób wizytujących.
4. **ADMINISTRATIVE DATA**	Wypełnia KWB/WWB.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Należy podać pełną nazwę oraz adres pocztowy. W tym należy wskazać odpowiednio miasto, państwo i kod pocztowy.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Należy podać pełną nazwę oraz adres pocztowy. W tym należy wskazać miasto, państwo, kod pocztowy, numer teleksu lub faksu (w stosownych przypadkach), numer telefonu i adres poczty elektronicznej. Należy podać imię i nazwisko oraz numer telefonu/faksu i adres poczty elektronicznej swojego głównego punktu kontaktowego lub osoby, z którą umówiono się na wizytę. Uwagi: 1) Podanie prawidłowego kodu pocztowego jest istotne, ponieważ przedsiębiorstwo może posiadać kilka różnych obiektów. 2) Podczas składania wniosku w formie papierowej można użyć załącznika 1, jeżeli wizyta ma obejmować co najmniej dwa obiekty w związku z tą samą sprawą. Jeżeli wykorzystywany jest załącznik, w pkt 3 należy napisać: „ZOB. ZAŁĄCZNIK 1, LICZBA OBIEKTÓW: …" (należy podać liczbę obiektów).
7. **DATES OF VISIT**	Należy podać dokładną datę lub zakres dat (od–do), w których ma się odbyć wizyta w formacie „dzień – miesiąc – rok". W stosownych przypadkach należy w nawiasie wskazać datę lub zakres dat, w których ma się odbyć kolejna wizyta.
8. **TYPE OF INITIATIVE**	Należy określić, czy wizyta ma się odbyć na prośbę organizacji wnioskującej lub obiektu wnioskującego, czy też na zaproszenie obiektu wizytowanego.
9. **THE VISIT RELATES TO:**	Należy podać pełną nazwę projektu, umowy lub zaproszenia do składania ofert, stosując jedynie powszechnie używane skróty.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Należy podać krótkie uzasadnienie powodu (powodów) wizyty. Nie należy używać nieobjaśnionych skrótów. Uwagi: W przypadku powtarzających się wizyt, w punkcie tym należy wpisać „Powtarzające się wizyty" jako pierwsze słowa w tym elemencie danych (np. Powtarzające się wizyty celem omówienia_____).
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Odpowiednio zgłosić SECRET UE/EU SECRET (S-UE/EU-S) lub CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C).
12. **PARTICULARS OF VISITOR**	Uwaga: jeżeli jest więcej osób wizytujących niż dwie, należy użyć załącznika 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	W tej pozycji należy podać imię i nazwisko, numer telefonu, numer faksu i adres poczty elektronicznej pełnomocnika ochrony obiektu wnioskującego.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Wypełnia instytucja certyfikująca. Uwagi dla instytucji certyfikującej: a) Należy podać imię i nazwisko, adres, numer telefonu, numer faksu i adres poczty elektronicznej (dopuszcza się wcześniejsze wydrukowanie). b) b. Punkt ten należy podpisać i opatrzyć pieczęcią (w stosownych przypadkach).
15. **REQUESTING SECURITY AUTHORITY**	Wypełnia KWB/WWB. Uwagi dla KWB/WWB: a) Należy podać imię i nazwisko, adres, numer telefonu, numer faksu i adres poczty elektronicznej (dopuszcza się wcześniejsze wydrukowanie). b) b. Punkt ten należy podpisać i opatrzyć pieczęcią (w stosownych przypadkach).

Należy wypełnić wszystkie pola i złożyć formularz wniosku za pośrednictwem kanałów międzyrządowych ([2]).

([2]) Jeżeli uzgodniono, że wizyty obejmujące dostęp lub potencjalny dostęp do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET można organizować bezpośrednio, wypełniony formularz można złożyć bezpośrednio do pełnomocnika ochrony obiektu, w którym planowana jest wizyta.

REQUEST FOR VISIT

(MODEL)

To: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided)*:

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Symbol zastępczy odniesienia do mających zastosowanie przepisów dotyczących danych osobowych oraz linku do obowiązkowych informacji dla osoby, której dane dotyczą, np. sposobu wdrażania art. 13 ogólnego rozporządzenia o ochronie danych ([3]).>

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Symbol zastępczy odniesienia do mających zastosowanie przepisów dotyczących danych osobowych oraz linku do obowiązkowych informacji dla osoby, której dane dotyczą, np. sposobu wdrażania art. 13 ogólnego rozporządzenia o ochronie danych ([1]).>

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

FIRMA/ORGANIZACJA:

(Należy kontynuować stosownie do potrzeb)

<Symbol zastępczy odniesienia do mających zastosowanie przepisów dotyczących danych osobowych oraz linku do obowiązkowych informacji dla osoby, której dane dotyczą, np. sposobu wdrażania art. 13 ogólnego rozporządzenia o ochronie danych ([1]).>

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

Dodatek D

ARKUSZ INFORMACYJNY DOTYCZĄCY ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

(MODEL)

1. **Wprowadzenie**

1.1. W załączeniu znajduje się przykładowy arkusz informacyjny dotyczący świadectwa bezpieczeństwa przemysłowego służący do szybkiej wymiany informacji między krajową władzą bezpieczeństwa (KWB) lub wyznaczoną władzą bezpieczeństwa (WWB), innymi właściwymi krajowymi organami ds. bezpieczeństwa i Komisją (jako instytucją zamawiającą) na temat świadectwa bezpieczeństwa przemysłowego (SBP) obiektu biorącego udział w niejawnych przetargach, będącego stroną niejawnych umów lub stroną niejawnych umów o podwykonawstwo.

1.2. Arkusz informacyjny dotyczący SBP jest ważny tylko wtedy, gdy nosi pieczęć właściwej KWB/WWB lub innego właściwego organu.

1.3. Arkusz informacyjny dotyczący SBP dzieli się na sekcję obejmującą wniosek i sekcję obejmującą odpowiedź i może być wykorzystywany do celów określonych powyżej lub do jakichkolwiek innych celów wymagających podania statusu SBP danego obiektu. KWB/WWB musi podać powód wniesienia zapytania w polu 7 sekcji dotyczącej wniosku.

1.4. Dane zamieszczone w arkuszu informacyjnym dotyczącym SBP są zazwyczaj jawne; dlatego też arkusze informacyjne dotyczące SBP powinny być przesyłane między odpowiednimi KWB/WWB/Komisją drogą elektroniczną.

1.5. KWB/WWB powinny dołożyć wszelkich starań, aby odpowiedzieć na wniosek zawarty w arkuszu informacyjnym dotyczącym SBP w terminie dziesięciu dni roboczych.

1.6. Gdyby w związku z tym zapewnieniem miały zostać przekazane informacje niejawne lub zawarta umowa w sprawie zamówienia publicznego, należy powiadomić wydającą KWB/WWB.

Procedury i instrukcje dotyczące wypełniania arkusza informacyjnego dotyczącego świadectwa bezpieczeństwa przemysłowego

Poniższe dokładne instrukcje przeznaczone są dla KWB/WWB lub instytucji zamawiającej Komisji, która wypełnia arkusz informacyjny dotyczący SBP. Najlepiej jest wypełnić wniosek wielkimi literami.

NAGŁÓWEK	Wnioskodawca podaje pełną nazwę KWB/WWB oraz państwa.
1. **RODZAJ WNIOSKU**	Wnioskująca instytucja zamawiająca wybiera pole wyboru odpowiadające wnioskowi zawartemu w arkuszu informacyjnym dotyczącym SBP. Należy uwzględnić stopień poświadczenia bezpieczeństwa, którego dotyczy wniosek. Należy stosować następujące skróty: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = system teleinformatyczny do przetwarzania informacji niejawnych

2. **DANE PODMIOTU**	Zawartość pól 1–6 jest oczywista. W polu 4 należy podać standardowy dwuliterowy kod. Pole 5 jest opcjonalne.
3. **POWÓD ZŁOŻENIA WNIOSKU**	Należy podać konkretny powód składania wniosku, wskaźniki projektu, numer umowy lub zaproszenia do składania ofert. Należy określić potrzeby w zakresie przechowywania, poziom klauzuli tajności CIS itp. Należy uwzględnić wszelkie terminy/daty upływu ważności/daty przyznania, które mogą mieć wpływ na zakończenie procedury wydawania SBP.
4. **WNIOSKUJĄCA KWB/WWB**	Należy podać imię i nazwisko faktycznego wnioskodawcy (w imieniu KWB/WWB) oraz datę złożenia wniosku w formacie liczbowym (dd/mm/rrrr).
5. **SEKCJA DOTYCZĄCA ODPOWIEDZI**	Pola 1–5: należy wybrać odpowiednie pola. Pole 2: jeżeli procedura wydawania SBP jest w toku, zaleca się, aby podać wnioskodawcy czas potrzebny na przetworzenie wniosku (jeżeli jest znany). Pole 6: a) Chociaż walidacja różni się w zależności od państwa lub nawet obiektu, zaleca się podanie daty upływu ważności SBP. b) W przypadku gdy zapewnienie SBP jest ważne na czas nieokreślony, można wykreślić to pole. c) Zgodnie z odpowiednimi przepisami i rozporządzeniami krajowymi wnioskodawca lub wykonawca albo podwykonawca odpowiada za złożenie wniosku o wznowienie SBP.
6. **UWAGI**	Można tu zamieścić dodatkowe informacje na temat SBP, obiektu lub poprzednich punktów.
7. **WYDAJĄCA KWB/WWB**	Należy podać imię i nazwisko organu wydającego (w imieniu KWB/WWB) oraz datę odpowiedzi w formacie liczbowym (dd/mm/rrrr).

ARKUSZ INFORMACYJNY DOTYCZĄCY ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

(MODEL)

Należy wypełnić wszystkie pola i przekazać formularz za pośrednictwem kanałów międzyrządowych lub między rządem i organizacją międzynarodową.

WNIOSEK O ZAPEWNIENIE ŚWIADECTWA BEZPIECZEŃSTWA PRZEMYSŁOWEGO

To: _____

(Nazwa państwa KWB/WWB)

W stosownych przypadkach należy wypełnić odpowiednie pola:

[] wydanie zapewnienia SBP na poziomie: [] S-UE/EU-S [] C-UE/EU-C

dla obiektu wymienionego poniżej

[] w tym ochrona materiałów/informacji niejawnych

[] w tym system teleinformatyczny (CIS) służący do przetwarzania informacji niejawnych

[] rozpoczęcie, bezpośrednie lub na odpowiedni wniosek wykonawcy lub podwykonawcy, procesu uzyskiwania SBP do poziomu ..... włącznie, z ochroną na poziomie ..... i CIS na poziomie ....., jeżeli obiekt nie dysponuje obecnie takimi poziomami zdolności.

Należy potwierdzić prawidłowość danych obiektu wymienionego poniżej i, w razie potrzeby, wprowadzić zmiany/dodatkowe informacje.

1. Pełna nazwa obiektu:	Zmiany/dodatkowe informacje:
.....	.....
2. Pełny adres obiektu:	
.....	.....
3. Adres pocztowy (jeżeli inny niż w pkt 2)	
.....	.....
4. Kod pocztowy	
.....	.....
5. Imię i nazwisko pełnomocnika ochrony	
.....	.....
6. Numer telefonu/numer faksu/adres poczty elektronicznej pełnomocnika ochrony	
.....	.....

7. Powód (powody) złożenia niniejszego wniosku: (należy podać dane dotyczące etapu przed zawarciem umowy (wyboru wariantu), umowy lub umowy o podwykonawstwo, programu/projektu itp.)

.....

Wnioskująca instytucja zamawiająca KWB/WWB/Komisji: Nazwa: ..... Data: (dd/mm/rrrr) .....

ODPOWIEDŹ (w terminie dziesięciu dni roboczych)

Niniejszym zaświadcza się, że:

1. [] powyższy obiekt posiada SBP do poziomu [] S-UE/EU-S włącznie

   [] C-UE/EU-C włącznie.

2. Powyższy obiekt jest zdolny do ochrony informacji/materiałów niejawnych:

   [] tak, na poziomie: ..... [] nie.

3. powyższy obiekt posiada akredytowany/zatwierdzony CIS:

   [] tak, na poziomie: ..... [] nie.

4. [] w odpowiedzi na powyższy wniosek rozpoczęto proces przyznawania SBP. Zostaną Państwo powiadomieni o przyznaniu lub odmowie przyznania SBP.

5. [] powyższy obiekt nie posiada SBP.

6. Niniejsze zapewnienie SBP wygasa w dniu: ..... (*dd/mm/rrrr*) lub w dniu określonym przez KWB/WWB. Zostaną Państwo powiadomieni w przypadku wcześniejszego unieważnienia informacji zamieszczonych powyżej lub jakichkolwiek ich zmian.

7. Uwagi:

   .....

Wydająca KWB/WWB Nazwa: ..... Data: *(dd/mm/rrrr)* .....

<Symbol zastępczy odniesienia do mających zastosowanie przepisów dotyczących danych osobowych oraz linku do obowiązkowych informacji dla osoby, której dane dotyczą, np. sposobu wdrażania art. 13 ogólnego rozporządzenia o ochronie danych ([2]).>

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

Dodatek E

Minimalne wymogi dotyczące ochrony EUCI w formie elektronicznej z klauzulą tajności RESTREINT UE/EU RESTRICTED przetwarzanych przez CIS wykonawcy

Warunki ogólne

1. Na wykonawcy musi spoczywać odpowiedzialność za zapewnienie, aby ochrona informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED spełniała minimalne wymogi bezpieczeństwa określone w niniejszej klauzuli dotyczącej bezpieczeństwa oraz wszelkie pozostałe wymogi dodatkowe zalecane przez instytucję zamawiającą lub w stosownych przypadkach przez krajową władzę bezpieczeństwa (KWB) lub wyznaczoną władzę bezpieczeństwa (WWB).

2. Na wykonawcy spoczywa odpowiedzialność za wdrożenie wymogów bezpieczeństwa określonych w niniejszym dokumencie.

3. Do celów niniejszego dokumentu system teleinformatyczny (CIS) obejmuje wszystkie urządzenia używane do wykorzystywania, przechowywania i przekazywania EUCI, w tym stacje robocze, drukarki, kopiarki, faksy, serwery, systemy zarządzania siecią, sterowniki sieciowe i sterowniki komunikacji, laptopy, notebooki, tablety, smartfony i przenośne urządzenia pamięciowe, m.in. pamięć USB, płyty CD, karty SD itp.

4. Specjalne urządzenia, takie jak produkty kryptograficzne, muszą być chronione zgodnie z dedykowanymi procedurami bezpiecznej eksploatacji systemu (SecOP).

5. Wykonawcy muszą utworzyć strukturę odpowiedzialną za zarządzanie bezpieczeństwem CIS, w których korzysta się z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, i wyznaczyć pełnomocnika ochrony odpowiedzialnego za dany obiekt.

6. Zabrania się użytkowania rozwiązań IT (sprzętu, oprogramowania lub usług) stanowiących własność prywatną pracowników wykonawcy do celów przechowywania lub przetwarzania informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED.

7. Akredytację CIS wykonawcy, w których korzysta się z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, musi potwierdzić organ ds. akredytacji bezpieczeństwa (SAA) danego państwa członkowskiego lub zadanie przeprowadzenia takiej akredytacji musi zostać powierzone pełnomocnikowi ochrony wykonawcy, jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość.

8. Jedynie informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED, które zostały zaszyfrowane przy użyciu zatwierdzonych produktów kryptograficznych, mogą być wykorzystywane, przechowywane lub przekazywane (przewodowo lub bezprzewodowo) podobnie jak wszelkie inne informacje jawne wynikające z umowy. Takie produkty kryptograficzne musi zatwierdzić UE lub państwo członkowskie.

9. Obiekty zewnętrzne wykorzystywane przy pracach konserwacyjnych/naprawach muszą być umownie zobowiązane do przestrzegania mających zastosowanie przepisów dotyczących korzystania z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, jak określono w niniejszym dokumencie.

10. Na wniosek instytucji zamawiającej lub odpowiednich KWB/WWB/SAA wykonawca musi przedstawić dowody na przestrzeganie klauzuli umownej dotyczącej bezpieczeństwa. Jeżeli wniosek dotyczy również przeprowadzenia audytu i kontroli procesów i obiektów wykonawcy w celu zapewnienia zgodności z tymi wymogami, wykonawcy zezwalają przedstawicielom instytucji zamawiającej, KWB/WWB/SAA lub odpowiedniego organu ds. bezpieczeństwa UE na przeprowadzenie takiego audytu i takiej kontroli.

Bezpieczeństwo fizyczne

11. Strefy, w których CIS wykorzystuje się do wyświetlania, przechowywania, przetwarzania lub przekazywania informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, lub strefy, w których znajdują się serwery, systemy zarządzania siecią, sterowniki sieciowe i sterowniki komunikacji dla takich CIS, muszą stanowić odrębne, kontrolowane strefy, w których stosuje się odpowiedni system kontroli dostępu. Dostęp do tych odrębnych, kontrolowanych stref powinny mieć jedynie osoby posiadające specjalne upoważnienie. Nie naruszając przepisów pkt 8, sprzęt opisany w pkt 3 należy przechowywać w takich odrębnych, kontrolowanych strefach.

12. Należy wdrożyć mechanizmy lub procedury bezpieczeństwa regulujące wprowadzanie lub podłączanie przenośnych komputerowych nośników danych (w tym pamięci USB, urządzeń pamięci masowej lub płyt CD-RW) do elementów CIS.

Dostęp do CIS

13. Dopuszcza się dostęp do CIS wykonawcy, w których korzysta się z EUCI, wyłącznie na zasadzie ograniczonego dostępu i uwierzytelnienia pracowników.

14. W odniesieniu do wszystkich CIS należy prowadzić aktualne wykazy upoważnionych użytkowników. Wszyscy użytkownicy muszą przejść proces uwierzytelnienia za każdym razem, gdy rozpoczynają sesję przetwarzania.

15. Hasła, które stanowią element większości środków bezpieczeństwa w zakresie potwierdzenia tożsamości i uwierzytelnienia, muszą składać się co najmniej z dziewięciu znaków, wśród których oprócz liter muszą znajdować się cyfry i znaki specjalne (jeżeli pozwala na to system). Hasła należy zmieniać co najmniej co 180 dni. Hasła należy zmieniać jak najszybciej w sytuacji, w której przestają być bezpieczne lub zostaną ujawnione osobie nieupoważnionej, lub w przypadku podejrzenia, że mogło dojść do takiej sytuacji.

16. Wszystkie CIS muszą posiadać wewnętrzne środki kontroli dostępu, aby uniemożliwić nieupoważnionym użytkownikom uzyskanie dostępu lub wprowadzenie zmian do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED oraz wprowadzenie zmian do środków kontroli systemu i bezpieczeństwa. Użytkownicy zostają automatycznie wylogowani z CIS, jeżeli ich terminale pozostawały nieaktywne przez wcześniej określony czas, lub po 15 minutach braku aktywności CIS musi aktywować wygaszacz ekranu chroniony hasłem.

17. Każdy użytkownik CIS otrzymuje unikalne konto użytkownika i identyfikator użytkownika. Konto użytkownika musi zostać automatycznie zablokowane po co najmniej pięciu kolejnych nieudanych próbach logowania.

18. Wszyscy użytkownicy CIS muszą zostać powiadomieni o obowiązkach i procedurach, których muszą przestrzegać w celu ochrony informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED wykorzystywanych w CIS. Użytkownicy muszą pisemnie potwierdzić, że zapoznali się z obowiązkami i procedurami, których należy przestrzegać, a obowiązki te i procedury muszą być udokumentowane.

19. Użytkownicy i administratorzy muszą mieć dostęp do procedur bezpiecznej eksploatacji systemu, które muszą obejmować opisy ról zabezpieczeń i powiązany wykaz zadań, instrukcji i planów.

Odpowiedzialność, audyt i reagowanie na zdarzenia

20. Aby uzyskać dostęp do CIS, należy każdorazowo zalogować się.

21. Należy rejestrować następujące zdarzenia:

    a) wszystkie próby logowania, zarówno udane, jak i nieudane;

    b) zdarzenia wylogowania (w tym w stosownych przypadkach z powodu upływu limitu czasu);

    c) tworzenie, usuwanie lub zmiany praw i uprawnień dostępu;

    d) tworzenie, usuwanie lub zmiany haseł.

22. W przypadku wszystkich wyżej wymienionych zdarzeń należy wskazać co najmniej następujące informacje:

    a) typ zdarzenia;

    b) ID użytkownika;

    c) datę i godzinę;

    d) ID urządzenia.

23. Zapisy aktywności powinny pomóc pełnomocnikowi ochrony w analizie potencjalnych zdarzeń naruszających bezpieczeństwo. Jeżeli dojdzie do zdarzenia naruszającego bezpieczeństwo, zapisy te mogą być przydatne w razie wszelkich postępowań prawnych. Wszystkie zapisy dotyczące bezpieczeństwa powinny być regularnie sprawdzane w celu identyfikacji potencjalnych zdarzeń naruszających bezpieczeństwo. Zapisy aktywności muszą być zabezpieczone przed nieuprawnionym usunięciem lub nieuprawnioną zmianą.

24. Wykonawca musi posiadać ustaloną strategię reagowania na zdarzenia naruszające bezpieczeństwo. Użytkowników i administratorów należy poinstruować, jak mają reagować na zdarzenia, jak je zgłaszać i co robić w sytuacji awaryjnej.

25. Naruszenie bezpieczeństwa lub podejrzenie naruszenia bezpieczeństwa w przypadku informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED należy zgłaszać instytucji zamawiającej. Zgłoszenie musi zawierać opis informacji, których bezpieczeństwo zostało naruszone, oraz opis okoliczności naruszenia lub podejrzewanego naruszenia. Wszyscy użytkownicy CIS muszą wiedzieć, w jaki sposób należy zgłaszać pełnomocnikowi ochrony każde faktyczne lub podejrzewane zdarzenie naruszające bezpieczeństwo.

Tworzenie sieci kontaktów i połączenia międzysystemowe

26. Jeżeli CIS wykonawcy, w którym wykorzystuje się informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED, jest połączony z CIS nieposiadającym akredytacji, fakt ten znacząco zwiększa zagrożenie zarówno dla bezpieczeństwa CIS, jak i dla bezpieczeństwa informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED wykorzystywanych w takim CIS. Dotyczy to internetu oraz innych publicznych lub prywatnych CIS, w tym innych CIS należących do danego wykonawcy lub podwykonawcy. W takim przypadku wykonawca musi przeprowadzić ocenę ryzyka w celu zidentyfikowania dodatkowych wymogów bezpieczeństwa, które należy wdrożyć w ramach procesu akredytacji bezpieczeństwa. Wykonawca przekazuje instytucji zamawiającej i, jeżeli jest to wymagane w krajowych przepisach ustawowych i wykonawczych, właściwemu SAA stwierdzenie o zgodności poświadczające, że CIS wykonawcy i jego połączenia międzysystemowe otrzymały akredytację do przetwarzania EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED.

27. Zdalny dostęp z innych systemów do usług LAN (np. zdalny dostęp do poczty elektronicznej i zdalna obsługa systemu) jest zabroniony, chyba że w porozumieniu z instytucją zamawiającą wdrożono specjalne środki bezpieczeństwa, które – jeżeli wymagają tego krajowe przepisy ustawowe i wykonawcze – zostały zatwierdzone przez właściwy SAA.

Zarządzanie konfiguracją

28. Należy zapewnić dostęp do szczegółowej konfiguracji sprzętu i oprogramowania, jak określono w dokumentacji dotyczącej akredytacji/zatwierdzenia (w tym schemat systemu/sieci) i jej regularną obsługę.

29. Pełnomocnik ochrony wykonawcy musi dokonywać kontroli konfiguracji sprzętu i oprogramowania w celu zapewnienia, aby nie doszło do nieuprawnionego wprowadzenia sprzętu lub oprogramowania.

30. Zmiany konfiguracji CIS wykonawcy muszą być oceniane pod kątem wpływu na zabezpieczenia oraz zatwierdzane przez pełnomocnika ochrony oraz – jeżeli wymagają tego krajowe przepisy ustawowe i wykonawcze – przez SAA.

31. Co najmniej raz na kwartał system należy skanować pod kątem wszelkich luk w zabezpieczeniach. Należy zainstalować i aktualizować oprogramowanie wykrywające złośliwe oprogramowanie. W miarę możliwości powinno ono posiadać krajowy certyfikat lub uznany certyfikat międzynarodowy, a w przeciwnym razie powinno stanowić powszechnie uznany standard branżowy.

32. Wykonawca musi opracować plan ciągłości działania. Konieczne jest ustanowienie procedur awaryjnych dotyczących:

    a) częstotliwości tworzenia kopii zapasowych;

    b) wymogów w zakresie przechowywania na miejscu (ogniotrwałe pojemniki) lub poza obiektem;

    c) kontroli uprawnionego dostępu do kopii zapasowych.

Czyszczenie i niszczenie

33. CIS lub nośniki danych, na których kiedykolwiek znajdowały się informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED, należy czyścić w następujący sposób stosowany do całego systemu lub nośnika danych przed ich usunięciem:

    a) dane w pamięci flash (np. pamięć USB, karty SD, dysk SSD, dysk hybrydowy) muszą zostać nadpisane co najmniej trzykrotnie – po czym należy przeprowadzić weryfikację, aby mieć pewność, że odzyskanie oryginalnej zawartości pamięci jest niemożliwe – lub usunięte za pomocą zatwierdzonego oprogramowania do usuwania danych;

    b) dane na nośnikach magnetycznych (np. dyskach twardych) muszą zostać nadpisane lub nośniki te należy poddać demagnetyzacji;

c) nośniki optyczne (np. płyty CD i DVD) należy zniszczyć w niszczarce lub rozdrobnić;

d) w przypadku wszelkich pozostałych nośników danych należy skonsultować się z instytucją zamawiającą lub, w stosownych przypadkach, z KWB/WWB/SAA w sprawie wymogów bezpieczeństwa, które należy spełnić.

34. Wszelkie nośniki danych należy oczyścić z informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED zanim zostaną przekazane jakiemukolwiek podmiotowi nieuprawnionemu do uzyskania dostępu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED (np. do celów konserwacyjnych).

ZAŁĄCZNIK IV

Świadectwo bezpieczeństwa przemysłowego i poświadczenie bezpieczeństwa osobowego w przypadku wykonawców w odniesieniu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED oraz KWB/WWB, które należy powiadomić o umowach niejawnych obejmujących informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED ([1])

Państwo członkowskie	SBP		Powiadomienie KWB/WWB o umowie lub umowie o podwykonawstwo obejmującej informacje z klauzulą tajności R-UE/EU-R		PBO	
	TAK	NIE	TAK	NIE	TAK	NIE
Belgia		X		X		X
Bułgaria		X		X		X
Republika Czeska		X		X		X
Dania	X		X		X	
Niemcy		X		X		X
Estonia	X		X			X
Irlandia		X		X		X
Grecja	X			X	X	
Hiszpania		X	X			X
Francja		X		X		X
Chorwacja		X	X			X
Włochy		X	X			X
Cypr		X	X			X
Łotwa		X		X		X

([1]) Te wymogi krajowe dotyczące SBP/PBO i powiadomień o umowach obejmujących informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED nie mogą nakładać żadnych dodatkowych obowiązków na inne państwa członkowskie ani na podlegających ich jurysdykcji wykonawców.
Uwaga: powiadamianie o umowach obejmujących informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET jest obowiązkowe.

Państwo członkowskie	SBP		Powiadomienie KWB/WWB o umowie lub umowie o podwykonawstwo obejmującej informacje z klauzulą tajności R-UE/EU-R		PBO	
	TAK	NIE	TAK	NIE	TAK	NIE
Litwa	X		X			X
Luksemburg	X		X		X	
Węgry		X		X		X
Malta		X		X		X
Niderlandy	X (dotyczy wyłącznie umów związanych z obronnością)		X (dotyczy wyłącznie umów związanych z obronnością)			X
Austria		X		X		X
Polska		X		X		X
Portugalia		X		X		X
Rumunia		X		X		X
Słowenia	X		X			X
Słowacja	X		X			X
Finlandia		X		X		X
Szwecja	X (dotyczy wyłącznie umów związanych z obronnością)		X (dotyczy wyłącznie umów związanych z obronnością)		X (dotyczy wyłącznie umów związanych z obronnością)	
Zjednoczone Królestwo		X		X		X

ZAŁĄCZNIK V

WYKAZ KRAJOWYCH WŁADZ BEZPIECZEŃSTWA/WYZNACZONYCH DZIAŁÓW WŁADZ BEZPIECZEŃSTWA ODPOWIEDZIALNYCH ZA PROWADZENIE PROCEDUR ZWIĄZANYCH Z BEZPIECZEŃSTWEM PRZEMYSŁOWYM

BELGIA

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tel. +32 25014542 (Sekretariat)
Faks +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BUŁGARIA

1. State Commission on Information Security - National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel. +359 29835775
   Faks +359 29873750
   E-mail: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel. +359 29227002
   Faks +359 29885211
   E-mail: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel. +359 29813221
   Faks +359 29862706
   E-mail: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel. +359 29824971
   Faks +359 29461339
   E-mail: dato@dato.bg

   (Wyżej wymienione właściwe organy przeprowadzają postępowanie sprawdzające na potrzeby wydawania SBP osobom prawnym ubiegającym się o zawarcie umowy niejawnej oraz PBO osobom fizycznym wykonującym umowę niejawną na potrzeby tych organów.)

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel. +359 28147109
   Faks +359 29632188, +359 28147441
   E-mail: dans@dans.bg

   (Wyżej wymienione służby bezpieczeństwa przeprowadzają postępowanie sprawdzające na potrzeby wydawania SBP i PBO wszystkim pozostałym osobom prawnym i osobom fizycznym w państwie, ubiegającym się o zawarcie lub wykonanie umowy niejawnej.)

CZECHY

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tel. +420 257283129
E-mail: sbr@nbu.cz

DANIA

1. Politiets Efterretningstjeneste
(Duńska Służba Wywiadowcza ds. Bezpieczeństwa)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Faks +45 33430190

2. Forsvarets Efterretningstjeneste
(Duńska Służba Wywiadowcza ds. Obrony)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Faks +45 33931320

NIEMCY

1. Kwestie dotyczące polityki bezpieczeństwa przemysłowego, SBP, planów przewozu (z wyjątkiem produktów kryptograficznych/poufnych informacji handlowych):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division - ZB3
Villemombler Str. 76
53123 Bonn
Tel. +49 228996154028
Faks +49 228996152676
E-mail: dsagermany-zb3@bmwi.bund.de (adres e-mail biura)

2. Standardowe wnioski w sprawie wizyty ze strony przedsiębiorstw niemieckich/w przedsiębiorstwach niemieckich:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Tel. +49 228996152401
Faks +49 228996152603
E-mail: zb2-international@bmwi.bund.de (adres e-mail biura)

3. Plany przewozu dotyczące materiałów kryptograficznych:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Tel. +49 2289995826052
Faks +49 228991095826052
E-mail: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tel. +372 6939211
Faks +372 6935001
E-mail: nsa@fis.gov.ee

IRLANDIA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tel. +353 14082724
E-mail: nsa@dfa.ie

GRECJA

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Tel. +30 2106572022, +30 2106572178
Faks +30 2106527612
E-mail: daa.industrial@hndgs.mil.gr

HISZPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel. +34 913725000
Faks +34 913725808
E-mail: nsa-sp@areatec.com
W kwestiach dotyczących poświadczeń bezpieczeństwa osobowego: asip@areatec.com
Odnośnie do planów przewozu i wizyt międzynarodowych: sp-ivtco@areatec.com

FRANCJA

Krajowa władza bezpieczeństwa (KWB) (w odniesieniu do polityki i wdrażania w dziedzinach innych niż obronność)
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 07 SP
Tel. +33 171758193
Faks +33 171758200
E-mail: ANSFrance@sgdsn.gouv.fr

Wyznaczona władza bezpieczeństwa (w odniesieniu do wdrażania w dziedzinie obronności)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15
Tel. +33 988670421
E-mail: formularze i wychodzące wnioski w sprawie wizyty: dga-ssdi.ai.fct@intradef.gouv.fr
przychodzące wnioski w sprawie wizyty: dga-ssdi.visit.fct@intradef.gouv.fr

CHORWACJA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel. +385 14681222
Faks +385 14686049
E-mail: NSACroatia@uvns.hr

WŁOCHY

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma
Tel. +39 0661174266
Faks +39 064885273

CYPR

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
E-mail: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Tel. +357 22807569, +357 22807764
Faks +357 22302351
E-mail: cynsa@mod.gov.cy

ŁOTWA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Tel. +371 67025418, +371 67025463
Faks +371 67025454
E-mail: ndi@sab.gov.lt, ndi@zd.gov.lv

LITWA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(Komisja Koordynacji Ochrony Informacji Niejawnych Republiki Litwy)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 70666703, +370 70666701
Faks +370 70666700
E-mail: nsa@vsd.lt

LUKSEMBURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tel. +352 24782210
E-mail: ans@me.etat.lu

WĘGRY

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 13911862
Faks +36 13911889
E-mail: nbf@nbf.hu

MALTA

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Tel.: +356 23952000
Faks +356 21242406
E-mail: certification@mccaa.org.mt

NIDERLANDY

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Tel. +31 703204400
Faks +31 703200733
E-mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Tel. +31 704419407
Faks +31 703459189
E-mail: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Tel. +43 153115202594
E-mail: isk@bka.gv.at

2. WWB w branży wojskowej:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
E-mail: abwa@bmlvs.gv.at

POLSKA

Agencja Bezpieczeństwa Wewnętrznego
Departament Ochrony Informacji Niejawnych
ul. Rakowiecka 2A
00-993 Warszawa
Tel. +48 225857944
Faks +48 225857443
E-mail: nsa@abw.gov.pl

PORTUGALIA

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel. +351 213031710
Faks +351 213031711
E-mail: sind@gns.gov.pt, franco@gns.gov.pt

RUMUNIA

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Rumuńska krajowa władza bezpieczeństwa – ORNISS – National Registry Office for Classified Information)
4th Mures Street
012275 Bucharest
Tel. +40 212075115
Faks +40 212245830
E-mail: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SŁOWENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Faks +386 14781399
E-mail: gp.uvtp@gov.si

SŁOWACJA

Národný bezpečnostný úrad
(Krajowa władza bezpieczeństwa)
Departament Poświadczania Bezpieczeństwa
Budatínska 30
851 06 Bratislava
Tel. +421 268691111
Faks +421 268691700
E-mail: podatelna@nbu.gov.sk

FINLANDIA

Krajowa władza bezpieczeństwa
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
E-mail: NSA@formin.fi

SZWECJA

1. Krajowa władza bezpieczeństwa
   Utrikesdepartementet (Ministerstwo Spraw Zagranicznych)
   UD SÄK/KWB
   SE-103 39 Stockholm
   Tel. +46 84051000
   Faks +46 87231176
   E-mail: ud-nsa@gov.se

2. WWB
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel. +46 87824000
   Faks +46 87826900
   E-mail: security@fmv.se

ZJEDNOCZONE KRÓLESTWO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel. +44 2072765497, +44 2072765645
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk