

Bruksela, 29 marca 2022 r.
(OR. en)

Międzyinstytucjonalny numer
referencyjny:
2022/0084(COD)

7670/22
ADD 5

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2022) 119 final - Annex 5
Dotyczy:	ZAŁĄCZNIKI do wniosku dotyczącego ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie bezpieczeństwa informacji w instytucjach, organach, urządach i agencjach Unii

Delegacje otrzymują w załączeniu dokument COM(2022) 119 final - Annex 5.

Załącznik: COM(2022) 119 final - Annex 5



KOMISJA
EUROPEJSKA

Bruksela, dnia 22.3.2022 r.
COM(2022) 119 final

ANNEX 5

ZAŁĄCZNIKI

do

**Wniosku dotyczącego ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I
RADY**

**w sprawie bezpieczeństwa informacji w instytucjach, organach, urządach i agencjach
Unii**

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ZAŁĄCZNIK V

Ochrona informacji niejawnych UE („EUCI”) w umowach niejawnych i niejawnych umowach o udzielenie dotacji

Do celów niniejszego załącznika oprócz definicji zawartych w załącznikach II i IV „świadczenie bezpieczeństwa przemysłowego” lub „SBP” oznacza oświadczenie wydane w trybie administracyjnym przez krajową władzę bezpieczeństwa, wyznaczoną władzę bezpieczeństwa lub jakiegokolwiek inny właściwy organ bezpieczeństwa, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiedni poziom ochrony EUCI do określonego poziomu klauzuli tajności.

Dostęp pracowników wykonawców i beneficjentów do EUCI

1. Każda instytucja lub każdy organ Unii, jako instytucja zamawiająca lub udzielająca dotacji, zapewnia, aby umowy niejawne lub niejawne umowy o udzielenie dotacji zawierały postanowienia wskazujące, że pracownicy wykonawcy, podwykonawcy lub beneficjent, którzy do wykonania umowy niejawnej, niejawnej umowy o podwykonawstwo lub niejawnej umowy o udzielenie dotacji potrzebują dostępu do EUCI, mogą uzyskać taki dostęp wyłącznie wtedy, gdy spełnione są następujące warunki:
 - a) ustalono, że pracownicy ci kierują się zasadą ograniczonego dostępu;
 - b) otrzymali od krajowej władzy bezpieczeństwa, wyznaczonej władzy bezpieczeństwa lub jakiegokolwiek innego właściwego organu bezpieczeństwa poświadczenie bezpieczeństwa osobowego („PBO”) do odpowiedniego poziomu informacji 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 beneficjent zamierza zatrudnić obywatela państwa trzeciego na stanowisku wymagającym dostępu do EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, zadaniem beneficjenta 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.

Świadczenie bezpieczeństwa przemysłowego („SBP”)

3. Świadczenie bezpieczeństwa przemysłowego („SBP”) wydawane jest przez krajową władzę bezpieczeństwa, wyznaczoną władzę bezpieczeństwa lub jakiegokolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego w celu zaświadczenia, że zgodnie z krajowymi przepisami ustawowymi i wykonawczymi dany podmiot jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET).
4. Jeżeli SBP jest wymagane do wykonania umowy lub umowy o udzielenie dotacji, instytucja lub organ Unii, jako instytucja zamawiająca lub udzielająca dotacji, musi powiadomić za pośrednictwem swojego organu ds. bezpieczeństwa odpowiednią

krajową władzę bezpieczeństwa lub wyznaczoną władzę bezpieczeństwa, lub jakiegokolwiek inny właściwy organ bezpieczeństwa.

5. SBP jest wymagane, jeżeli podczas postępowania o udzielenie zamówień lub podczas procedury przyznawania dotacji informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET mają być dostarczone do obiektów kandydatów, oferentów lub wnioskodawców.
6. Instytucja lub organ Unii, jako instytucja zamawiająca lub udzielająca dotacji, musi przed udzieleniem dostępu do EUCI kandydatowi, oferentowi lub wykonawcy bądź wnioskodawcy lub beneficjentowi otrzymać, za pośrednictwem swojego organu ds. bezpieczeństwa, ich potwierdzenie SBP.
7. W przypadku gdy państwa członkowskie nie wydają SBP określonym instytucjom na podstawie przepisów prawa krajowego, instytucja zamawiająca lub udzielająca dotacji musi sprawdzić u danej krajowej władzy bezpieczeństwa lub wyznaczonej władzy bezpieczeństwa, czy te instytucje są w stanie korzystać z EUCI na wymaganym poziomie.
8. Z wyjątkiem przypadków, o których mowa w pkt 7, instytucja lub organ Unii, jako instytucja zamawiająca lub udzielająca dotacji, nie może zawrzeć umowy niejawnej lub niejawnej umowy o udzielenie dotacji przed otrzymaniem potwierdzenia za pośrednictwem swojego organu ds. bezpieczeństwa, od właściwej krajowej władzy bezpieczeństwa, wyznaczonej władzy bezpieczeństwa lub jakiegokolwiek innego właściwego krajowego organu bezpieczeństwa, że odpowiednie SBP zostało wydane.
9. Cofnięcie SBP przez odpowiednią krajową władzę bezpieczeństwa/wyznaczoną władzę bezpieczeństwa lub jakiegokolwiek inny właściwy organ bezpieczeństwa stanowi dla instytucji zamawiającej lub udzielającej dotacji wystarczający powód do rozwiązania umowy niejawnej lub niejawnej umowy o udzielenie dotacji bądź wykluczenia kandydata, oferenta lub wnioskodawcy z postępowania.

Przepisy dotyczące przetargów oraz realizacji umów niejawnych i niejawnych umów o udzielenie dotacji

10. Jeżeli kandydatowi, oferentowi lub wnioskodawcy podczas postępowania o udzielenie zamówień publicznych lub procedury wyboru przekazywane są EUCI, zaproszenie do składania ofert lub zaproszenie do składania wniosków musi zawierać postanowienie zobowiązujące kandydata, oferenta lub wnioskodawcę, który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.
11. Od wykonawcy lub beneficjenta dotacji wymaga się z reguły zwrotu wszelkich posiadanych przez niego EUCI do instytucji zamawiającej lub udzielającej dotacji po rozwiązaniu umowy niejawnej lub niejawnej umowy o udzielenie dotacji lub po zakończeniu uczestnictwa przez beneficjenta dotacji.
12. Przepisy szczegółowe dotyczące usuwania EUCI podczas wykonywania umowy niejawnej lub niejawnej umowy o udzielenie dotacji bądź po jej rozwiązaniu muszą zostać ustanowione w dokumencie określającym aspekty bezpieczeństwa.
13. Jeżeli wykonawca lub beneficjent dotacji są upoważnieni do zachowania EUCI po rozwiązaniu umowy niejawnej lub niejawnej umowy o udzielenie dotacji, wykonawca lub beneficjent dotacji muszą nadal przestrzegać minimalnych

standardów zawartych w niniejszym rozporządzeniu oraz nadal chronić poufność EUCI.

14. W zaproszeniu do składania ofert lub w zaproszeniu do składania wniosków oraz w umowie niejawnnej lub niejawnnej umowie o udzielenie dotacji muszą być określone istotne dla ochrony EUCI warunki, na których wykonawca lub beneficjent może zlecić podwykonawstwo.
15. Przed zleceniem podwykonawstwa którejkolwiek części umowy niejawnnej lub niejawnnej umowy o udzielenie dotacji wykonawca lub beneficjent musi uzyskać zgodę instytucji zamawiającej lub udzielającej dotacji.
16. Wykonawca lub beneficjent musi odpowiadać za zapewnienie zgodności wszystkich podejmowanych w ramach podwykonawstwa czynności z minimalnymi normami określonymi w niniejszym rozporządzeniu i nie może dostarczać EUCI podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej lub udzielającej dotacji.
17. Jeżeli chodzi o EUCI wytworzone przez wykonawcę lub beneficjenta, instytucja lub organ Unii będące instytucją zamawiającą lub udzielającą dotacji są uznawane za ich wytwórcę i wykonują prawa przysługujące wytwórcy.
18. Jeżeli na podstawie krajowych przepisów ustawowych i wykonawczych państwa członkowskie wymagają posiadania SBP lub poświadczenia bezpieczeństwa osobowego w odniesieniu do umów, umów o udzielenie dotacji lub umów o podwykonawstwo na poziomie RESTREINT UE/EU RESTRICTED, instytucje i organy Unii, jako instytucje zamawiające lub udzielające dotacji, nie mogą wykorzystywać tych wymogów krajowych, aby nakładać dodatkowe obowiązki na pozostałe państwa członkowskie ani aby wykluczać oferentów, wnioskodawców, wykonawców, beneficjentów lub podwykonawców z państw członkowskich, w których nie obowiązują takie wymogi dotyczące SBP lub poświadczenia bezpieczeństwa osobowego w zakresie dostępu do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, z wykonania powiązanych umów, umów o udzielenie dotacji lub umów o podwykonawstwo lub z procedury ubiegania się o takie umowy.

Wizyty związane z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji

19. Jeżeli w kontekście wykonania umowy niejawnnej lub niejawnnej umowy o udzielenie dotacji instytucjom i organom Unii, wykonawcom, beneficjentom lub podwykonawcom niezbędny jest dostęp do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w ich obiektach, we współpracy z krajowymi władzami bezpieczeństwa, wyznaczonymi władzami bezpieczeństwa lub jakimkolwiek innymi właściwymi organami bezpieczeństwa muszą zostać zorganizowane wizyty.
20. Wizyty, o których mowa w pkt 19, podlegają następującym wymogom:
 - a) wizyta musi być przeprowadzana w celach oficjalnych związanych z umową niejawną lub niejawną umową o udzielenie dotacji;
 - b) każda osoba wizytująca musi posiadać poświadczenie bezpieczeństwa osobowego na wymaganym poziomie i kierować się zasadą ograniczonego dostępu do EUCI wykorzystywanych lub generowanych w toku realizacji umowy niejawnnej lub niejawnnej umowy o udzielenie dotacji;

- c) co najmniej 15 dni przed datą wizyty właściwej dla obiektu krajowej władzy bezpieczeństwa lub wyznaczonej władzy bezpieczeństwa, lub organowi ds. bezpieczeństwa danej instytucji lub danego organu Unii musi zostać przedłożony formalny wniosek o wizytę.
21. W kontekście konkretnych projektów właściwa krajowa władza bezpieczeństwa lub wyznaczona władza bezpieczeństwa i organ ds. bezpieczeństwa danej instytucji lub danego organu Unii mogą uzgodnić procedurę, zgodnie z którą pełnomocnik ochrony osoby wizytującej i pełnomocnik ochrony wizytowanego obiektu mogą bezpośrednio organizować wizyty dotyczące konkretnej umowy lub dotacji niejawnnej. Taka szczególna procedura musi być określona w instrukcji bezpieczeństwa programu lub projektu lub w ramach innego rodzaju szczególnych ustaleń.
22. Wizyty obejmujące dostęp do informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED muszą być organizowane bezpośrednio między podmiotami wysyłającymi i wizytowanymi.

Przekazywanie EUCI drogą elektroniczną w związku z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji

23. Elektroniczne przetwarzanie i przekazywanie EUCI musi odbywać się zgodnie z rozdziałem 5 sekcja 5.

Systemy teleinformatyczne będące własnością wykonawcy, beneficjenta lub podwykonawcy i używane do przetwarzania i przechowywania EUCI na potrzeby wykonania umowy lub umowy o udzielenie dotacji muszą podlegać akredytacji przez odpowiedzialny organ ds. akredytacji bezpieczeństwa (SAA) państwa lub organizacji międzynarodowej, w ramach właściwości których funkcjonuje wykonawca, beneficjent lub podwykonawca.

Wszelkie przekazywanie EUCI drogą elektroniczną w kontekście umów niejawnych i niejawnych umów o udzielenie dotacji musi podlegać ochronie przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 42.

24. Akredytację bezpieczeństwa CIS wykonawców lub beneficjentów, w którym przetwarza się EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED, oraz jakichkolwiek jego połączeń międzysystemowych można zlecić pełnomocnikowi ochrony wykonawcy lub beneficjenta, jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość.

Jeżeli zadanie akredytacji bezpieczeństwa zostaje zlecone podwykonawcy, wykonawca lub beneficjent musi odpowiadać za wdrożenie wymogów bezpieczeństwa opisanych w dokumencie określającym aspekty bezpieczeństwa przy przetwarzaniu informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED za pomocą CIS. Odpowiednie krajowe władze bezpieczeństwa lub krajowe władze bezpieczeństwa oraz SAA pozostają odpowiedzialne za ochronę informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED, które przetwarza lub przechowuje wykonawca lub beneficjent, i zachowują prawo do kontroli środków bezpieczeństwa wprowadzonych przez wykonawcę lub beneficjenta.

Ponadto wykonawca lub beneficjent musi przekazać instytucji lub organowi Unii, jako instytucji zamawiającej lub udzielającej dotacji, a jeżeli jest to wymagane zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, właściwemu krajowemu SAA, stwierdzenie zgodności poświadczające, że CIS wykonawcy lub beneficjenta i związane z nim połączenia międzysystemowe otrzymały akredytację

do przetwarzania i przechowywania EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED.

Osobiste przenoszenie EUCI w związku z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji

25. Osobiste przenoszenie informacji niejawnych związane z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji musi podlegać rygorystycznym wymogom bezpieczeństwa.
26. Pracownicy wykonawcy lub beneficjenta w Unii Europejskiej 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;
 - b) EUCI przez cały czas znajdują się w posiadaniu osoby je przenoszącej;
 - c) koperta lub opakowanie nie są otwierane, dopóki osoba przenosząca nie dotrze do swojego miejsca przeznaczenia.
27. W odniesieniu do informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET warunki osobistego przenoszenia przez pracowników wykonawcy lub beneficjenta na terenie państwa członkowskiego 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 oraz imię i nazwisko kuriera. 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 na wewnętrznej kopercie
 - c) EUCI przez cały czas znajdują się w posiadaniu osoby je przenoszącej;
 - d) koperta lub opakowanie nie są otwierane, dopóki osoba przenosząca nie dotrze do swojego miejsca przeznaczenia;
 - e) koperta lub opakowanie są przenoszone w aktówce wyposażonej w zamek lub w podobnym zatwierdzonym pojemniku o takim rozmiarze i masie, że może on przez cały czas znajdować się w posiadaniu osoby go przenoszącej;
 - f) kurier ma przy sobie list kurierski wydany przez właściwy organ bezpieczeństwa, któremu podlega, upoważniający kuriera do przewozu wskazanej przesyłki niejawnej.
28. W przypadku osobistego przenoszenia informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przez pracowników wykonawcy lub beneficjenta z jednego państwa członkowskiego do innego oprócz wymogów określonych w pkt 27 zastosowanie mają następujące przepisy dodatkowe:
 - a) kurier odpowiada za bezpieczne przechowanie materiałów niejawnych do momentu ich przekazania odbiorcy;

- b) w przypadku naruszenia bezpieczeństwa krajowa władza bezpieczeństwa lub wyznaczona władza bezpieczeństwa 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 musi zostać powiadomiony o wszystkich obowiązkach dotyczących bezpieczeństwa, których należy przestrzegać podczas przenoszenia informacji, i podpisać stosowne oświadczenia;
- d) do listu kurierskiego załączona zostaje instrukcja przeznaczona dla kuriera;
- e) kurier musi otrzymać opis przesyłki i trasy podróży;
- f) list kurierski i powiązane dokumenty muszą zostać zwrócone wydającej je krajowej władzy bezpieczeństwa lub wyznaczonej władzy bezpieczeństwa po zakończeniu podróży lub odbiorca listu kurierskiego przechowuje je i udostępnia do celów monitorowania;
- g) jeżeli organy celne, imigracyjne lub policja graniczna zażądają okazania przesyłki do kontroli, należy im zezwolić na otwarcie i zobaczenie 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, powinno to się odbywać 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 zabezpieczowania przesyłki i pisemnego potwierdzenia, że przesyłka została otwarta przez te organy.

29. Osobiste przenoszenie przez pracowników wykonawcy lub beneficjenta informacji z klauzulą tajności SECRET UE/EU SECRET do państwa trzeciego lub do organizacji międzynarodowej podlega postanowieniom umowy o bezpieczeństwie informacji zawartej między Unią Europejską a takim państwem trzecim albo taką organizacją międzynarodową.

Transport EUCI przez kurierów komercyjnych i jako ładunek w związku z umowami niejawnymi i niejawnymi umowami o udzielenie dotacji

30. Transport EUCI przez kurierów komercyjnych musi odbywać się zgodnie z odpowiednimi przepisami załącznika IV.
31. W przypadku transportu materiałów niejawnych jako ładunku do określania zabezpieczeń muszą być stosowane następujące zasady:
- a) na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do miejsca przeznaczenia, musi być zapewnione bezpieczeństwo;
 - b) stopień ochrony, którym objęto przesyłkę, musi być określany według najwyższego poziomu klauzuli tajności materiałów zawartych w przesyłce;

- c) przedsiębiorstwa dokonujące przewozu muszą uzyskać SBP na stosownym poziomie. W takich przypadkach pracownicy zajmujący się przesyłką muszą zostać odpowiednio sprawdzeni;
- d) przed jakimkolwiek transgranicznym przewożeniem materiałów z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET nadawca musi sporządzić plan przewozu, który jest zatwierdzany przez krajową władzę bezpieczeństwa, wyznaczoną władzę bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa;
- e) przejazdy muszą odbywać się w miarę możliwości bezpośrednio między dwoma punktami i kończyć się tak szybko, jak pozwolą na to okoliczności;
- f) jeżeli jest to możliwe, trasy muszą przebiegać wyłącznie przez terytoria państw członkowskich. Transport trasami przebiegającymi przez terytoria państw trzecich musi się odbywać wyłącznie pod warunkiem zatwierdzenia przez krajową władzę bezpieczeństwa, wyznaczoną władzę bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa zarówno państwa nadawcy, jak i państwa odbiorcy.