

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

Międzyinstytucjonalny numer
referencyjny:
2022/0084 (COD)

7670/22
ADD 3

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

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	22 marca 2022 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2022) 119 final - Annex 3
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 3.

Zał.: COM(2022) 119 final - Annex 3



KOMISJA
EUROPEJSKA

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

ANNEX 3

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 III

Środki służące fizycznej ochronie informacji niejawnych UE („EUCI”)

Sprzęt i środki organizacyjne służące fizycznej ochronie EUCI

1. Strefa administracyjna musi spełniać następujące wymagania:
 - a) wyraźnie określona musi być jej granica umożliwiająca kontrolę osób i, jeżeli to możliwe, pojazdów;
 - b) należy zapewnić, aby okna, które mogłyby umożliwić wizualny dostęp podmiotom nieuprawnionym do EUCI znajdujących się w tej strefie, były nieprzezroczyste lub wyposażone w żaluzje, zasłony lub inne osłony;
 - c) dostęp bez eskorty przyznaje się tylko osobom, które są odpowiednio upoważnione przez organ ds. bezpieczeństwa danej instytucji lub danego organu Unii;
 - d) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.
2. Oprócz wymogów określonych w pkt 1 strefa bezpieczeństwa musi spełniać następujące wymogi:
 - a) wyraźnie określone i chronione muszą być jej granice, których przekraczanie w obie strony jest kontrolowane przez cały czas;
 - b) nie mogą się w niej znajdować niezatwierdzone linie komunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny;
 - c) musi być wyposażona w system kontroli dostępu i system sygnalizacji włamania i napadu w czasie rzeczywistym („SSWiN”) obsługiwany przez pracowników ochrony odpowiedzialnych za bezpieczeństwo;
 - d) musi być poddawana inspekcji na koniec normalnych godzin pracy i w przypadkowych odstępach czasu poza tymi godzinami, jeżeli w strefie tej nie pracują w systemie całodobowym pracownicy pełniący dyżur ani nie ma w niej SSWiN monitorującego w czasie rzeczywistym;
 - e) muszą nią zarządzać przeszkoleni, nadzorowani i odpowiednio sprawdzeni pracownicy ochrony;
 - f) w strefie bezpieczeństwa muszą obowiązywać procedury bezpiecznej eksploatacji, obejmujące następujące elementy:
 - (i) poziom klauzuli tajności EUCI, które można wykorzystywać, omawiać i przechowywać w tej strefie;
 - (ii) środki nadzoru i ochrony, które należy stosować;
 - (iii) osoby upoważnione do wejścia do strefy bez eskorty ze względu na posiadane upoważnienie do dostępu do EUCI i zasadę ograniczonego dostępu;
 - (iv) w odpowiednich przypadkach procedury dotyczące eskort lub ochrony EUCI, jeżeli zezwala się na wejście do strefy innym osobom;
 - (v) wszelkie inne odpowiednie środki i procedury.

3. Jeżeli wejście do strefy bezpieczeństwa jest równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie, strefę tę należy uznać za strefę klasy I, a w przeciwnym razie – za strefę klasy II.

W przypadku obu klas strefy bezpieczeństwa, o których mowa w akapicie pierwszym, oraz w uzupełnieniu wymogów określonych w pkt 2, departament bezpieczeństwa / pełnomocnik ochrony danej instytucji lub danego organu Unii musi wyraźnie określić najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie, oraz musi wyraźnie określić granicę umożliwiającą kontrolę osób i, jeżeli to możliwe, pojazdów.

Instytucje i organy Unii muszą zapewnić, aby osoby mające dostęp do strefy bezpieczeństwa spełniały następujące kryteria:

- a) muszą posiadać specjalne upoważnienie do wejścia do tej strefy;
 - b) przez cały czas musi im towarzyszyć eskorta;
 - c) muszą być odpowiednio sprawdzone, chyba że podjęte zostały kroki służące zapewnieniu, aby dostęp do EUCI był niemożliwy.
4. Za strefę technicznie zabezpieczoną musi być uznana strefa bezpieczeństwa chroniona przed podsłuchem pasywnym i aktywnym. Oprócz wymogów dotyczących stref bezpieczeństwa obowiązują następujące wymogi:
- a) strefy takie muszą być wyposażone w SSWiN, zamknięte na klucz, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa. Zarządzanie wszystkimi kluczami odbywa się zgodnie z art. 29 ust. 3;
 - b) muszą być poddawane regularnym inspekcjom fizycznym lub technicznym lub obu rodzajom inspekcji, przeprowadzanym przez organ ds. bezpieczeństwa danej instytucji lub danego organu Unii. Inspekcje takie muszą być przeprowadzane także po każdorazowym nieuprawnionym wejściu do strefy lub w przypadku podejrzenia, że takie wejście miało miejsce;
 - c) muszą posiadać odpowiednią ochronę akustyczną i ochronę TEMPEST.
5. Wszystkie osoby wchodzące do stref technicznie zabezpieczonych muszą spełniać wymogi określone w pkt 3.
6. Strefy bezpieczeństwa oraz strefy technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu.
7. W obrębie stref bezpieczeństwa muszą być budowane wzmocnione pomieszczenia. Wzmocnione pomieszczenie to pomieszczenie o wzmocnionej konstrukcji fizycznej, w którym organ ds. bezpieczeństwa danej instytucji lub danego organu Unii zatwierdza ściany, podłogi, sufity, okna i wyposażone w zamek drzwi. Pomieszczenia takie zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI o tym samym poziomie klauzuli tajności.

Fizyczne środki ochronne dotyczące korzystania z EUCI i ich przechowywania

8. Wykorzystywanie i przetwarzanie EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED musi się odbywać w którejkolwiek z następujących stref:
- a) w strefie bezpieczeństwa;

- b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych;
 - c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz zobowiązał się do zastosowania środków równoważnych określonych przez organ ds. bezpieczeństwa każdej instytucji i każdego organu Unii.
9. EUCI z klauzulą tajności RESTREINT UE/EU RESTRICTED muszą być przechowywane w zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. Mogą być one tymczasowo przechowywane poza strefą administracyjną lub strefą bezpieczeństwa, pod warunkiem że posiadacz zobowiązał się do przechowywania danych dokumentów w odpowiednim zamkniętym meblu biurowym, gdy nie są one czytane ani omawiane.
10. Instytucje i organy Unii mogą wykorzystywać i przechowywać informacje z klauzulą tajności RESTREINT UE/EU RESTRICTED poza swoimi siedzibami, pod warunkiem że istotne informacje są odpowiednio chronione. W tym celu instytucje i organy Unii muszą stosować środki określone w pkt 8 lit. c).
11. Wykorzystywanie i przechowywanie informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET musi odbywać się w jednej z następujących stref:
- a) w strefie bezpieczeństwa;
 - b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych;
 - c) poza strefą bezpieczeństwa lub strefą administracyjną, w przypadku gdy ich ilość i czas wykorzystywania i przechowywania są ograniczone oraz pod warunkiem, że posiadacz zobowiązał się do zastosowania środków równoważnych określonych przez organ ds. bezpieczeństwa danej instytucji lub danego organu Unii. Ponadto posiadacz EUCI musi podjąć następujące działania:
 - (i) powiadamia odpowiednią kancelarię o fakcie, że z dokumentów niejawnych korzysta się poza strefami chronionymi;
 - (ii) zapewnia, aby dokumenty znajdowały się przez cały czas pod jego kontrolą.
12. Informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET muszą być przechowywane w strefie bezpieczeństwa akredytowanej na tym poziomie tajności przez właściwy organ ds. akredytacji bezpieczeństwa danej instytucji lub danego organu Unii, w zabezpieczonej szafie albo we wzmocnionym pomieszczeniu.
13. Dokumenty z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą mogą być kopiowane tylko przez odpowiednią kancelarię.
14. Wykorzystywanie i przechowywanie informacji z klauzulą tajności TRES SECRET UE/EU TOP SECRET musi odbywać się w strefie bezpieczeństwa posiadającej akredytację dotyczącą tego poziomu klauzuli tajności. W tym celu instytucje i organy Unii mogą dokonać niezbędnych ustaleń, aby korzystać ze strefy bezpieczeństwa wizytowanej i akredytowanej na odpowiednim poziomie tajności przez organ ds. akredytacji bezpieczeństwa innej instytucji i innego organu Unii.

15. Informacje z klauzulą tajności TRES SECRET UE/EU TOP SECRET muszą być przechowywane w strefie bezpieczeństwa akredytowanej na tym poziomie tajności przez organ ds. akredytacji bezpieczeństwa właściwej instytucji lub właściwego organu Unii, przy spełnieniu jednego z następujących warunków:
- a) są one przechowywane w zabezpieczonej szafie zatwierdzonej przez organ ds. bezpieczeństwa każdej instytucji i każdego organu Unii, której towarzyszy co najmniej jedno z następujących zabezpieczeń dodatkowych:
 - (i) stała ochrona lub kontrola przez odpowiednio sprawdzonych pracowników ochrony lub pracowników pełniących dyżur;
 - (ii) zatwierdzony SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo;
 - b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo.