ADDENDUM DO ZAPROSZEŃ DO WYRAŻENIA ZAINTERESOWANIA PRACĄ W CHARAKTERZE PRACOWNIKÓW KONTRAKTOWYCH

(1) Na stronie 2 sekcja 1 ustęp 1 otrzymuje brzmienie:

„1) Niniejsze zaproszenie do wyrażenia zainteresowania dotyczy następujących profili i grup funkcyjnych:

Lp.	Nr procedury	Profil	Grupa funkcyjna (GF)
1	EPSO/CAST/P/1/2017	Finanse	GF III
2	EPSO/CAST/P/2/2017	Finanse	GF IV
3	EPSO/CAST/P/3/2017	Zarządzanie projektami/programami	GF III
4	EPSO/CAST/P/4/2017	Zarządzanie projektami/programami	GF IV
5	EPSO/CAST/P/5/2017	Finanse	GF II
6	EPSO/CAST/P/6/2017	Pracownicy sekretariatu / Pracownicy biurowi	GF II
7	EPSO/CAST/P/7/2017	Administracja / Zasoby ludzkie	GF II
8	EPSO/CAST/P/8/2017	Administracja / Zasoby ludzkie	GF III
9	EPSO/CAST/P/9/2017	Administracja / Zasoby ludzkie	GF IV
10	EPSO/CAST/P/10/2017	Komunikacja	GF III
11	EPSO/CAST/P/11/2017	Komunikacja	GF IV
12	EPSO/CAST/P/12/2017	Sprawy polityczne / Polityka unijna	GF III
13	EPSO/CAST/P/13/2017	Sprawy polityczne / Polityka unijna	GF IV
14	EPSO/CAST/P/14/2017	Prawo	GF III
15	EPSO/CAST/P/15/2017	Prawo	GF IV
16	EPSO/CAST/P/16/2017	Technologie informacyjno-komunikacyjne	GF III
17	EPSO/CAST/P/17/2017	Technologie informacyjno-komunikacyjne	GF IV
18	EPSO/CAST/P/18/2017	Pracownicy do pomocniczych zadań fizycznych i administracyjnych	GF I
19	EPSO/CAST/P/19/2018	Pracownicy placówek opieki nad dziećmi	GF II
20	EPSO/CAST/P/20/2018	Psycholodzy szkolni	GF IV
21	EPSO/CAST/P/21/2019	Korektorzy tekstów	GF III
22	EPSO/CAST/P/22/2019	Tłumacze pisemni	GF IV
23	EPSO/CAST/P/23/2022	Zarządzanie budynkami – Pracownik ds. logistycznych i technicznych	GF II
24	EPSO/CAST/P/24/2022	Zarządzanie budynkami – Specjalista budowlany	GF III
25	EPSO/CAST/P/25/2022	Zarządzanie budynkami – Inżynier/architekt	GF IV
26	EPSO/CAST/P/26/2023	Działania w zakresie bezpieczeństwa, w tym bezpieczeństwa regionalnego	GF IV
27	EPSO/CAST/P/27/2023	Działania w zakresie bezpieczeństwa, w tym bezpieczeństwa regionalnego	GF III
28	EPSO/CAST/P/28/2023	Działania w zakresie bezpieczeństwa	GF II
29	EPSO/CAST/P/29/2023	Bezpieczeństwo techniczne	GF IV
30	EPSO/CAST/P/30/2023	Bezpieczeństwo techniczne	GF III
31	EPSO/CAST/P/31/2023	Bezpieczeństwo techniczne	GF II
32	EPSO/CAST/P/32/2023	Bezpieczeństwo informacji i dokumentów	GF IV
33	EPSO/CAST/P/33/2023	Bezpieczeństwo informacji i dokumentów	GF III
34	EPSO/CAST/P/34/2023	Bezpieczeństwo informatyczne	GF IV
35	EPSO/CAST/P/35/2023	Bezpieczeństwo informatyczne	GF III”

(2) Na końcu załącznika I „Typowy zakres obowiązków” należy dodać następujące sekcje:

„DZIAŁANIA W ZAKRESIE BEZPIECZEŃSTWA, W TYM BEZPIECZEŃSTWA REGIONALNEGO – GF IV

1. Pracownicy ds. bezpieczeństwa

1.1. Udział w opracowywaniu i rozwijaniu polityk bezpieczeństwa oraz wytycznych niezbędnych do ich wdrożenia.
1.2. Przygotowywanie i ułatwianie podejmowania decyzji (kierowniczych lub operacyjnych) w obszarze kompetencji departamentu.
1.3. Zarządzanie usługami bezpieczeństwa operacyjnego, ich wykonywanie i koordynowanie (w tym, w stosownych przypadkach, zarządzanie budżetem i umowami w dziedzinach takich jak umowy o ochronę lub inne aspekty związane z usługami bezpieczeństwa operacyjnego).
1.4. Administrowanie i kierowanie konkretnymi projektami.
1.5. Zarządzanie całodobowym podmiotem operacyjnym ds. reagowania w sytuacjach wyjątkowych lub dyspozytornią ochrony i bezpieczeństwa oraz koordynowanie ich działań.
1.6. Opracowywanie strategii i planów oraz koordynowanie działań podnoszących świadomość w zakresie bezpieczeństwa.
1.7. Nadzorowanie, motywowanie i koordynowanie zespołu i zarządzanie nim w celu jak najlepszego wykorzystania zasobów kadrowych i zapewnienia jakości usług.
1.8. Zarządzanie reagowaniem w sytuacjach wyjątkowych stanowiących potencjalne zagrożenie dla osób, mienia lub informacji.
1.9. Zarządzanie działaniami w zakresie bezpieczeństwa operacyjnego w dziedzinie kontrwywiadu, zwalczania terroryzmu i zarządzania kryzysowego oraz realizowanie tych działań.
1.10. Przeprowadzanie oceny zagrożeń i analizy ryzyka w dziedzinie bezpieczeństwa, w tym zalecanie i wdrażanie środków bezpieczeństwa.
1.11. Przeprowadzanie postępowań sprawdzających.
1.12. Organizowanie ochrony bezpośredniej VIP-ów.

2. Doradcy ds. bezpieczeństwa regionalnego

2.1. Opracowywanie, ocena i nadzorowanie użytkowania sprzętu oraz wdrażanie procedur bezpieczeństwa osób, mienia i informacji.
2.2. Zapewnianie dobrych kontaktów z władzami lub agencjami oraz nawiązywanie niezbędnych kontaktów ze społeczeństwem obywatelskim.
2.3. Udział w spotkaniach dotyczących bezpieczeństwa organizowanych przez państwa członkowskie, ONZ lub innych partnerów.
2.4. Wdrażanie środków w zakresie procedur zarządzania kryzysowego, obejmujących aspekty ewakuacji.
2.5. Zapewnianie określenia środków i podejmowanie działań następczych w związku z zaleceniami w dziedzinach bezpieczeństwa osób, mienia lub informacji.
2.6. Zapewnianie kompletności, terminowości i wykonalności planów awaryjnych delegatury oraz zapewnianie, by personel był poinformowany, a plany – przetestowane.
2.7. Zapewnianie przestrzegania procedur bezpieczeństwa w przypadku kryzysu w delegaturze UE (lub w biurze) w ramach kompetencji geograficznych oraz nadzorowanie aktualizacji list pracowników oddelegowanych za granicę i ich rodzin w przypadku ewakuacji.
2.8. Podnoszenie świadomości i szkolenie pracowników oddelegowanych za granicę i innych pracowników oraz doradzanie im w kwestiach ochrony i bezpieczeństwa.
2.9. Udział we wdrażaniu środków bezpieczeństwa oraz regularne informowanie głównej instytucji i szefów delegatur (lub biur) na obszarze geograficznym, za który doradca jest odpowiedzialny, za pomocą analizy sytuacji oraz sprawozdań ustnych i pisemnych.

2.10. Przygotowywanie i regularne aktualizowanie lokalnych ocen zagrożenia i ocen ryzyka dla bezpieczeństwa w krajach należących do obszaru geograficznego, za który doradca jest odpowiedzialny. Opracowywanie, ocena i nadzorowanie wdrażania środków zapobiegawczych i łagodzących.
2.11. Udział w przeglądzie i aktualizacji polityk, norm i procedur związanych z bezpieczeństwem.
2.12. Przeprowadzanie audytów bezpieczeństwa dotyczących konkretnych kwestii lub udział w takich audytach.

DZIAŁANIA W ZAKRESIE BEZPIECZEŃSTWA, W TYM BEZPIECZEŃSTWA REGIONALNEGO – GF III

1. Pracownicy ds. bezpieczeństwa

1.1. Udział w reagowaniu w sytuacjach wyjątkowych stanowiących potencjalne zagrożenie dla osób, mienia lub informacji.
1.2. Gromadzenie, organizowanie i analizowanie danych wywiadowczych na podstawie otwartego oprogramowania, baz danych i innych narzędzi informatycznych.
1.3. Przeprowadzanie oceny zagrożeń i analizy ryzyka w dziedzinie bezpieczeństwa, w tym sporządzanie zaleceń i wdrażanie środków bezpieczeństwa.
1.4 Wdrażanie i koordynowanie usług w zakresie bezpieczeństwa operacyjnego oraz usług nadzoru pracowników ochrony.
1.5. Koordynowanie całodobowych zespołów operacyjnych ds. reagowania w sytuacjach wyjątkowych lub dyspozytorów bezpieczeństwa i ochrony, przy zapewnieniu integralności funkcjonowania służb technologicznych i kontroli procesów technicznych.
1.6. Udział w badaniach, sporządzaniu notatek, podsumowań lub statystyk, przygotowywaniu projektów regulacyjnych.
1.7. Przygotowywanie i wdrażanie planów kryzysowych w zakresie bezpieczeństwa.
1.8. Przygotowanie i udział w operacyjnym zarządzaniu wydarzeniami.
1.9. Monitorowanie wdrażania przepisów dotyczących dostępu do budynków i korzystania z parkingów, egzekwowanie tych przepisów, stosowanie prewencji zgodnie z tymi przepisami.
1.10. Przeprowadzanie postępowań sprawdzających.
1.11. Przeprowadzanie inspekcji środków przeciwdziałania inwigilacji technicznej.
1.12. Świadczenie usług ochrony bezpośredniej VIP-ów.

2. Pracownicy ds. bezpieczeństwa regionalnego

2.1. Opracowywanie, ocena i nadzorowanie użytkowania sprzętu oraz wdrażanie procedur bezpieczeństwa osób, mienia i informacji.
2.2. Zapewnianie dobrych kontaktów z władzami lub agencjami oraz nawiązywanie niezbędnych kontaktów ze społeczeństwem obywatelskim.
2.3. Udział w spotkaniach dotyczących bezpieczeństwa organizowanych przez państwa członkowskie, ONZ lub innych partnerów.
2.4. Wdrażanie środków w dziedzinie procedur zarządzania kryzysowego, w tym aspektów ewakuacji.
2.5. Określanie środków technicznych i podejmowanie działań następczych w związku z zaleceniami w dziedzinie bezpieczeństwa osób, mienia lub informacji.
2.6. Zapewnianie kompletności, terminowości i wykonalności planów awaryjnych delegatury oraz zapewnianie, by personel był poinformowany, a plany – przetestowane.
2.7. Zapewnianie przestrzegania procedur bezpieczeństwa w przypadku kryzysu w delegaturze UE (lub w biurze) w ramach kompetencji geograficznych oraz nadzorowanie aktualizacji list pracowników oddelegowanych za granicę i ich rodzin w przypadku ewakuacji.

2.8. Podnoszenie świadomości i szkolenie pracowników oddelegowanych za granicę i innych pracowników oraz doradzanie im w kwestiach ochrony i bezpieczeństwa.
2.9. Udział we wdrażaniu środków bezpieczeństwa oraz regularne informowanie głównej instytucji i szefów delegatur (lub biur) na obszarze geograficznym, za który doradca jest odpowiedzialny, w drodze sprawozdań ustnych i pisemnych.
2.10. Przygotowywanie i regularne aktualizowanie lokalnych ocen zagrożenia i ocen ryzyka dla bezpieczeństwa w krajach należących do obszaru geograficznego, za który doradca jest odpowiedzialny. Opracowywanie, ocena i nadzorowanie wdrażania środków zapobiegawczych i łagodzących.

DZIAŁANIA W ZAKRESIE BEZPIECZEŃSTWA – GF II

1. Prowadzenie działań centrum ds. reagowania w sytuacjach wyjątkowych.
2. Obsługa i monitorowanie systemów i aplikacji bezpieczeństwa: systemów wczesnego ostrzegania, kontroli dostępu, systemów alarmowych i systemów CCTV, wykrywania wtargnięć, komunikacji radiowej itp.
3. Reagowanie na zdarzenia związane z bezpieczeństwem zgodnie z obowiązującymi instrukcjami.
4. Weryfikowanie jakości usług w zakresie bezpieczeństwa.
5. Sporządzanie raportów dotyczących incydentów, sporządzanie i monitorowanie raportów podsumowujących wydarzenia, anomalie i kontrole wykonane podczas świadczenia usług.
6. Udział w zarządzaniu ryzykiem w obszarze bezpieczeństwa.
7. Monitorowanie dostępu do wejść do budynków i sal posiedzeń, udział w nadzorze budynków i obiektów.
8. Udział w postępowaniach sprawdzających.
9. Świadczenie usług ochrony bezpośredniej VIP-ów.

BEZPIECZEŃSTWO TECHNICZNE – GF IV

1. Opracowywanie i wdrażanie specyfikacji technicznych lub procedur operacyjnych na podstawie oceny zagrożeń i analizy ryzyka.
2. Przygotowywanie, koordynowanie i opracowywanie projektów bezpieczeństwa technicznego oraz zarządzanie tymi projektami.
3. Formułowanie i udoskonalanie minimalnych standardów bezpieczeństwa technicznego.
4. Zarządzanie instalacją, nadzorowaniem działania, eksploatacją i utrzymaniem technicznych systemów bezpieczeństwa.

BEZPIECZEŃSTWO TECHNICZNE – GF III

1. Przeprowadzanie oceny ryzyka związanego z bezpieczeństwem technicznym i sporządzanie specyfikacji technicznych dotyczących projektów w zakresie bezpieczeństwa technicznego.
2. Monitorowanie robót budowlanych i instalacji w obszarze sprzętu bezpieczeństwa i ochrony.
3. Monitorowanie eksploatacji i utrzymania systemów i produktów bezpieczeństwa technicznego.

BEZPIECZEŃSTWO TECHNICZNE – GF II

1. Udział w analizie ryzyka związanego z bezpieczeństwem technicznym.
2. Monitorowanie robót budowlanych i instalacji dotyczących systemów i sprzętu w obszarze bezpieczeństwa i ochrony.
3. Monitorowanie eksploatacji i utrzymania systemów i produktów bezpieczeństwa technicznego.

BEZPIECZEŃSTWO INFORMACJI I DOKUMENTÓW – GF IV

1. Opracowywanie polityk bezpieczeństwa, norm i powiązanych dokumentów.
2. Projektowanie, analizowanie, opracowywanie i wdrażanie środków kontroli bezpieczeństwa dostosowanych do ocenianego poziomu ryzyka w obszarze bezpieczeństwa informacji i dokumentów.
3. Identyfikacja, ocena i integracja produktów związanych z bezpieczeństwem, w tym udoskonalenie konkretnych narzędzi bezpieczeństwa (między innymi wdrażanie rozwiązań opartych na otwartym oprogramowaniu w dziedzinie bezpieczeństwa informatycznego).
4. Opracowywanie procedur i systemów przetwarzania informacji niejawnych UE, projektowanie bezpiecznych usług administrowania i monitorowania systemu.

BEZPIECZEŃSTWO INFORMACJI I DOKUMENTÓW – GF III

1. Udział w opracowywaniu polityk i wdrażaniu kontroli bezpieczeństwa w dziedzinie bezpieczeństwa informacji i dokumentów.
2. Zapewnienie dobrego funkcjonowania usług mających na celu przetwarzanie informacji niejawnych UE, udział w rozwijaniu, administrowaniu i właściwym korzystaniu ze ściśle tajnych systemów łączności i informacji.

BEZPIECZEŃSTWO INFORMATYCZNE – GF IV

1. Opracowywanie polityk bezpieczeństwa, norm i powiązanych dokumentów.
2. Projektowanie, analizowanie, opracowywanie i wdrażanie środków kontroli bezpieczeństwa dostosowanych do ocenianego poziomu ryzyka w obszarze bezpieczeństwa informacji i dokumentów.
3. Identyfikacja, ocena i integracja produktów związanych z bezpieczeństwem, w tym udoskonalenie konkretnych narzędzi bezpieczeństwa (między innymi wdrażanie rozwiązań opartych na otwartym oprogramowaniu w dziedzinie bezpieczeństwa informatycznego).
4. Przeprowadzanie: okresowej oceny bezpieczeństwa, audytów bezpieczeństwa informatycznego, inspekcji bezpieczeństwa informatycznego, zarządzania podatnością na zagrożenia i oceny takiej podatności, testów penetracyjnych.
5. Wykrywanie incydentów związanych z bezpieczeństwem informatycznym, koordynowanie reagowania na incydenty związane z bezpieczeństwem informatycznym oraz postępowań sprawdzających w sprawie incydentów.

BEZPIECZEŃSTWO INFORMATYCZNE – GF III

1. Pomoc w opracowywaniu polityk bezpieczeństwa, norm i powiązanych dokumentów.
2. Pomoc w projektowaniu, analizowaniu, opracowywaniu i wdrażaniu środków kontroli bezpieczeństwa dostosowanych do ocenianego poziomu ryzyka w obszarze bezpieczeństwa informacji i dokumentów.
3. Pomoc w identyfikacji, ocenie i integracji produktów związanych z bezpieczeństwem, w tym udoskonaleniu konkretnych narzędzi bezpieczeństwa (między innymi wdrażanie rozwiązań opartych na otwartym oprogramowaniu w dziedzinie bezpieczeństwa informatycznego).
4. Pomoc w: okresowej ocenie bezpieczeństwa, audytach bezpieczeństwa informatycznego, inspekcjach bezpieczeństwa informatycznego, zarządzaniu podatnością na zagrożenia i ocenie takiej podatności, testach penetracyjnych.
5. Pomoc w wykrywaniu incydentów związanych z bezpieczeństwem informatycznym, koordynowaniu reagowania na incydenty związane z bezpieczeństwem informatycznym oraz postępowań sprawdzających w sprawie incydentów.

6. Przeprowadzanie specjalistycznych kontroli i postępowań sprawdzających dotyczących bezpieczeństwa informatycznego.”