|  |  |
| --- | --- |
| Numer sprawy: RIZP 271.21.2025 | Załącznik nr 1 do SWZ |
| Szczegółowy Opis Przedmiotu Zamówienia  pn. Przeprowadzenie szkoleń  dla administratorów IT | |

# Zestawienie ilościowe.

Przeprowadzenie szkoleń dla administratorów IT

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa | Ilość |
| 1. | Zakup usług szkolenia dla administratorów IT | 2 osoby |

# Termin realizacji zamówienia.

Zamówienie wykonać należy w terminach wskazanych w dokumentacji przetargowej.

# Opis przedmiotu zamówienia

# Zakup usług szkolenia dla administratorów IT

Wymagania ogólne dla szkoleń:

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 17.00.
4. Szkolenia będą prowadzone w języku polskim w trybie zdalnym w formule on-line. Zamawiający dopuszcza materiały w języku angielskim.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
7. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
8. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
9. W ramach organizacji szkoleń Wykonawca zapewni:
   1. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej lub elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto w przypadku organizacji szkoleń w formule stacjonarnej, uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie uczestnikom na własność 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
   2. Wykonawca jest zobowiązany dostarczyć narzędzia do komunikacji zdalnej, które umożliwią dwustronne przesyłanie przez sieć Internet obrazu i dźwięku między prowadzącym szkolenie a uczestnikami szkolenia. Narzędzie musi umożliwiać zadawanie pytań także w formie pisemnej bezpośrednio na czacie w trakcie trwania sesji szkoleniowej.
   3. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń w przypadku prowadzenia szkoleń stacjonarnych.
   4. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
   5. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
   6. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń. Wykonawca jest zobowiązany zapewnić kadrę trenerską posiadającą minimum dwuletnie doświadczenie w prowadzeniu szkoleń w obszarze którego dotyczy szkolenie.
   7. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
      * Lista obecności uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia).
      * Lista odbioru zaświadczeń o ukończeniu szkolenia.
      * Potwierdzenie przez uczestników odbioru materiałów szkoleniowych.
      * Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
      * Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

Zakres merytoryczny szkoleń:

Szkolenie powinno zostać podzielone na trzy moduły.

Moduł nr 1 – autoryzowane szkolenie CompTIA Cybersecurity Analyst (CySA+) wraz z przygotowaniem i zapewnieniem podejścia do egzaminu CS0-003 – rekomendowany program szkolenia:

1. Wprowadzenie do CySA+ i zarządzania bezpieczeństwem:
   1. Cybersecurity Leadership – role, obowiązki, komunikacja.
   2. Control Types and Methods – prewencyjne, detekcyjne, korekcyjne.
   3. Patch Management – planowanie, wdrażanie, ryzyko związane z łatami.
2. Wprowadzenie do wywiadu i rozpoznawania zagrożeń:
   1. Threat Intelligence & Threat Hunting – źródła, cykle życia, modele.
   2. Threat Actor Types – APT, skrypty, insiderzy, grupy przestępcze.
   3. Active Threats – jak je rozpoznać i jak reagować.
3. Architektura i bezpieczeństwo systemów:
   1. Network and System Architecture – komponenty, segmentacja, DMZ.
   2. Identity and Access Management (IAM) – AAA, SSO, MFA.
   3. Operational Visibility – monitorowanie, SIEM, logi.
4. Doskonalenie procesów operacyjnych:
   1. Process Improvement – metryki, KPI, ciągłe doskonalenie.
   2. Leadership in SecOps – zarządzanie zespołami i projektami.
   3. Security Technology Stack – przegląd narzędzi (EDR, NDR, DLP, itd.).
5. Skany podatności i zgodność:
   1. Implementing Vulnerability Scanning – skanery, harmonogramy, targety.
   2. Compliance Requirements – NIST, ISO, PCI-DSS, GDPR.
   3. Special Considerations – systemy przemysłowe, chmura, zdalni pracownicy.
6. Analiza i ocena podatności:
   1. Performing Vulnerability Analysis – interpretacja wyników skanów.
   2. Vulnerability Scoring – CVSS, kontekst organizacyjny.
   3. Communicating Vulnerability Info – raportowanie, rekomendacje, priorytetyzacji.
7. Planowanie i działania IR (Incident Response):
   1. Incident Response Activities – etapy IR: przygotowanie, wykrycie, reakcja itd.
   2. Incident Response Planning – playbooki, runbooki, symulacje.
   3. Performing IR – narzędzia, procedury, role zespołów.
8. Komunikacja w sytuacjach kryzysowych:
   1. Effective Communication – w czasie incydentu i po nim.
   2. Reporting Outcomes – dokumentacja, lessons learned.
   3. Action Plans – działania naprawcze i prewencyjne.
9. Wykrywanie i analiza złośliwej aktywności:
   1. Tools for Identifying Malicious Activity – IDS, SIEM, sandboxing.
   2. Attack Methodologies – MITRE ATT&CK, Cyber Kill Chain.
   3. Techniques for Analysis – korelacja, analiza heurystyczna.
10. Wskaźniki kompromitacji:
    1. Network Indicators – nietypowy ruch, skanowanie, tunelowanie.
    2. Host Indicators – logi, podejrzane procesy, zmiany w rejestrze.
    3. Analysis in Practice – case studies, analiza danych.
11. Analiza podatności aplikacji i chmury:
    1. Vulnerability Assessment Tools – dla aplikacji, hostów, środowisk cloud.
    2. Web & Cloud Vulnerabilities – OWASP Top 10, błędna konfiguracja, uprawnienia.
    3. Application Vulnerability Assessment – DAST, SAST, IAST.
12. Scripting i analiza złośliwego kodu:
    1. Scripting Tools – Python, Bash, PowerShell.
    2. Analysis Concepts – logika kodu, analiza malware, reverse engineering.
13. Zabezpieczanie aplikacji:
    1. Secure SDLC – DevSecOps, testowanie kodu.
    2. Mitigation Techniques – WAF, input validation, least privilege.

Moduł nr 2 – szkolenie CPENT AI: Certified Penetration Testing Professional wraz z przygotowaniem i zapewnieniem podejścia do egzaminu CPENT – rekomendowany program szkolenia:

1. Wprowadzenie do testów penetracyjnych i metodologii:
   1. Cele i zasady testów penetracyjnych.
   2. Metodologie EC-Council i LPT.
   3. Etyka, prawo i zarządzanie zakresem (ROE, NDA, kontrakty).
2. Planowanie i angażowanie klienta:
   1. Przygotowanie propozycji i harmonogramu.
   2. Określenie zakresu i celów testów.
   3. Zasady angażowania interesariuszy i zarządzania oczekiwaniami.
3. Open Source Intelligence (OSINT):
   1. Techniki zbierania informacji z publicznych źródeł
   2. Narzędzia OSINT (np. Maltego, Recon-ng, theHarvester)
   3. Mapowanie powierzchni ataku i analiza ryzyka
4. Inżynieria społeczna:
   1. Phishing, vishing, smishing, tailgating
   2. Techniki manipulacji i motywacji
   3. Przeciwdziałanie i raportowanie
5. Testowanie aplikacji webowych:
   1. OWASP Top 10 – testowanie i eksploatacja
   2. SQL Injection, XSS, CSRF, SSRF
   3. Testowanie API, JWT, sesji, uwierzytelniania i autoryzacji
6. Testowanie zewnętrzne:
   1. Rozpoznanie i skanowanie (Nmap, Nessus, Nikto)
   2. Eksploatacja usług i aplikacji
   3. Przechwytywanie i analiza ruchu
7. Testowanie wewnętrzne:
   1. Lateralne przemieszczanie się w sieci
   2. Eskalacja uprawnień (Windows/Linux)
   3. Ustalanie haseł, ataki na AD, SMB, RDP
8. Testowanie urządzeń peryferyjnych:
   1. Testowanie zapór, routerów, VPN, IDS/IPS
   2. Ataki na urządzenia sieciowe i IoT
   3. Techniki obejścia filtrów i firewalli
9. Testowanie IoT i OT/SCADA:
   1. Analiza urządzeń IoT i protokołów (Zigbee, BLE, MQTT)
   2. Testowanie systemów OT/SCADA (Modbus, DNP3, OPC)
   3. Przeciwdziałanie i raportowanie
10. Testowanie chmury:
    1. Testowanie środowisk AWS, Azure, GCP
    2. Analiza konfiguracji i uprawnień
    3. Testowanie aplikacji i baz danych w chmurze
11. Eksploatacja binarna i inżynieria wsteczna:
    1. Analiza i eksploatacja plików binarnych
    2. Fuzzing, buforowanie, przepełnienie stosu
    3. Narzędzia: GDB, IDA Pro, Radare2, AFL
12. Pisanie raportów i działania po testach:
    1. Struktura raportu pentestowego
    2. Dokumentowanie luk, dowodów i rekomendacji
    3. Prezentacja wyników klientowi i interesariuszom

Moduł nr 3 – szkolenie dotyczące zapewnienia cyberbezpieczeństwa dla Active Directory w kontekście dyrektywy NIS 2 – rekomendowany program szkolenia:

1. Regulacje prawne i cyberbezpieczeństwo w organizacji:
   1. Dyrektywa NIS2 – podstawy prawne i znaczenie.
   2. Bezpieczeństwo infrastruktury IT a zgodność z przepisami.
   3. Cyberzagrożenia i model warstwowej ochrony.
   4. Bezpieczeństwo personelu.
2. Zarządzanie dostępem i tożsamością w środowisku AD:
   1. Analiza ryzyka i wdrażanie polityk bezpieczeństwa dostępu
   2. Architektura uwierzytelniania – komponenty i procesy
   3. Zarządzanie kontami i strukturą AD
   4. Zasady minimalnych uprawnień i podział administracji.
   5. Bezpieczna administracja – narzędzia i praktyki.
3. Wzmacnianie i nadzorowanie infrastruktury Windows/AD:
   1. Zabezpieczenie kontrolerów domeny i usług towarzyszących.
   2. Zarządzanie zasadami GPO jako centralny mechanizm kontroli.
   3. Wdrożenie praktyk „hardeningu” dla środowisk Windows.
4. Monitorowanie, inspekcja i subskrypcja logów zdarzeń.
5. Ochrona danych, certyfikaty i kontrola transmisji
   1. Zabezpieczenie danych i mechanizmy szyfrowania.
   2. Infrastruktura klucza publicznego (PKI) – urzędy certyfikacji.
6. Transmisja zabezpieczona – SSL/TLS, IIS, IPSec.
   1. Zdalny dostęp, VPN, aktualizacje i stacje końcowe.
   2. Zdalne połączenia – bezpieczeństwo dostępu spoza organizacji.
   3. Aktualizacje i zarządzanie poprawkami – rola WSUS.
   4. Zabezpieczanie stacji końcowych z Windows 11.

Dodatkowe wymagania:

1. W ramach usługi zostaną przeszkolone 2 osoby z zastrzeżeniem, że jedna osoba bierze udział w nie więcej niż 2 modułach szkoleniowych.
2. Szkolenie powinno trwać minimum 105 godzin szkoleniowych, po 35 godzin szkoleniowych dla jednego modułu.
3. Zapewnienie egzaminów powinno umożliwiać podejście do egzaminu do w okresie trwania umowy, przewiduje się udział jednej osoby w jednym egzaminie.

# Równoważność rozwiązań.

1. Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
2. Zamawiający informuje, że tam, gdzie w Zapytaniu oraz załącznikach opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Zamawiający informuje, iż w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać materiały użyte do realizacji przedmiotu zamówienia. Ewentualne użycie nazwy producenta ma wyłącznie charakter przykładowy i ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania.
3. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.
4. Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji.

# Klauzula informacyjna FERC.

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

Administrator danych

Odrębnymi administratorami Państwa danych są:

1. Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
2. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
3. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego prawo (art. 6 ust. 1 lit. c RODO):

1) art. 87 ustawy wdrożeniowej,

2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),

3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),

4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),

5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,

6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405), Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,

1. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
2. Przygotowujemy i realizujemy umowy, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres zaangażowania w projekcie,
3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFiPR oraz CPPC. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
3. instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC;
4. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

Okres przechowywania danych

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy de minimis oraz przepisów dotyczących podatku od towarów i usług.

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),
3. do usunięcia swoich danych (art. 17 RODO) - jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO,
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

1. IOD MFiPR:

1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,

2) elektronicznie na adres e-mail: IOD@mfipr.gov.pl,

2. IOD CPPC:

1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,

2) elektronicznie na adres e-mail: bezpieczenstwo@cppc.gov.pl.

Podstawa prawna:

1. ustawa wdrożeniowa - ustawa z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r., poz. 1079),
2. RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i  w sprawie swobodnego przepływu takich danych (Dz. Urz. UE. L 119 z 4 maja 2016 r., s.1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).