OPIS PRZEDMIOTU ZAMÓWIENIA

na **“Przeprowadzenie kampanii cyberawereness oraz szkoleń z zakresu cyberbezpieczeństwa”.**

1 Wstęp

1.1 Cel zamówienia

Celem zamówienia jest kompleksowe podniesienie poziomu świadomości i kompetencji pracowników Urzędu Zamówień Publicznych w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem ograniczenia ryzyka ataków socjotechnicznych (phishing, smishing, ataki przez komunikatory) oraz wdrożenia nowoczesnych praktyk ochrony informacji. Program ma na celu trwałą zmianę postaw i nawyków użytkowników, budowę kultury bezpieczeństwa oraz zwiększenie odporności organizacji na zagrożenia związane z działalnością człowieka.

1.2 Kontekst projektu i źródła finansowania

Projekt realizowany jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności oraz programu „Cyberbezpieczny Rząd”, finansowanego ze środków NextGenerationEU. Stanowi element strategii bezpieczeństwa organizacji, mający na celu wzmocnienie infrastruktury teleinformatycznej oraz podniesienie kompetencji pracowników w zakresie cyberbezpieczeństwa.

1.3 Zakres czasowy i możliwość przedłużenia

Umowa zostanie zawarta na okres do 15. czerwca 2026. Zamawiający przewiduje prawo opcji, na warunkach określonych w dokumentacji zamówienia.

1.4 Zakres przedmiotu zamówienia

Przedmiot zamówienia obejmuje:

- Przeprowadzenie szkoleń stacjonarnych i zdalnych (webinarów) dla wszystkich pracowników oraz dedykowanych spotkań indywidualnych dla kierownictwa i dyrektorów.
- Organizację i realizację regularnych kampanii cyber awareness, w tym symulacji ataków phishingowych, smishingowych i przez komunikatory.
- Szkolenie z wykorzystania kluczy sprzętowych U2F (Yubikey) oraz follow-up szkoleniowy.

- Raportowanie, ewaluację działań edukacyjnych oraz wsparcie powdrożeniowe i konsultacje eksperckie.

2 Zakres przedmiotu zamówienia

2.1 Zakres ogólny

Przedmiot zamówienia obejmuje kompleksową realizację programu podnoszenia świadomości cyberbezpieczeństwa w Urzędzie Zamówień Publicznych, zorientowanego na trwałą zmianę postaw i nawyków pracowników oraz ograniczenie ryzyka ataków socjotechnicznych i wycieków danych. Program łączy działania edukacyjne, praktyczne oraz motywacyjne, obejmując wszystkie kluczowe grupy pracowników.

2.2 Zakres rzeczowy – podział na komponenty

2.2.1 Szkolenia stacjonarne i zdalne

- Realizacja szkoleń stacjonarnych w siedzibie zamawiającego (ul. Postępu 17a, Warszawa) obejmujących dwa cykle szkoleniowe dla w sumie 160 osób, w grupach do 40 osób, bez cateringu, w sali zapewnionej przez zamawiającego. Jedno szkolenie trwające maksymalnie 45 minut.
- Realizacja szkoleń zdalnych prowadzonych na platformie MS Teams zamawiającego, z możliwością zadawania pytań na żywo, nagrywane i archiwizowane przez zamawiającego.
- Szkolenia stacjonarne i zdalne realizowane zgodnie z 5.1 Struktura cyklu szkoleniowego.
- Szkolenia indywidualne dla nowych pracowników (do 10 szkoleń w okresie pół roku), realizowane zdalnie na żądanie, w dni robocze w godzinach pracy urzędu, z możliwością grupowania w przypadku kilku zgłoszeń w jednym tygodniu.
- Przewodnik po bezpieczeństwie (2 strony, elektronicznie) przekazywany każdemu nowemu pracownikowi.

2.2.2 Spotkania indywidualne dla kierownictwa i dyrektorów

- Spotkania 1:1 (stacjonarne) dla 5 osób z kierownictwa i 17 dyrektorów, trwające 45–60 minut, z przygotowaniem OSINT na temat uczestnika.
- Zakres spotkania obejmuje przekrojowe zagadnienia, analizę indywidualnych zagrożeń, czas na pytania indywidualne.

- Spotkania nie są dokumentowane, nie przewiduje się przekazywania materiałów podsumowujących.

2.2.3 Kampanie cyber awareness i symulacje ataków

- Regularne kampanie phishingowe, smishingowe (SMS) oraz przez komunikatory (MS Teams i inne popularne komunikatory), każda forma wykorzystana co najmniej dwukrotnie w okresie umowy.
- Kampania telefoniczna – vishing do trzech osób wskazanych przez Zamawiającego na etapie realizacji umowy
- 60% akcji targetowanych na całą organizację, 40% na wybrane grupy funkcyjne (w uzgodnieniu z zamawiającym).
- Szablony wiadomości każdorazowo zatwierdzane przez zamawiającego.
- Raporty z kampanii zawierają szczegółową analizę skuteczności szablonów, statystyki uczestnictwa, rekomendacje naprawcze dla grup z niskim zaangażowaniem oraz konsultacje z zespołem ds. bezpieczeństwa.

2.2.4 Materiały na Platformę szkoleniową

-
- Automatyczne, cotygodniowe mikro-lekcje (2–5 min), powiadomienia e-mail, segmentacja użytkowników według działów/roli.
- Raportowanie i analityka w podziale na segmenty użytkowników oraz ogólnie.
- Przechowywanie historii wszystkich kampanii i szkoleń przez cały okres trwania umowy oraz po jej zakończeniu (przez okres przejściowy).
- Personalizacja interfejsu zgodnie z identyfikacją wizualną zamawiającego.
- Platforma nie przechowuje nagrań webinarów/szkoleń (przechowywane na MS Teams zamawiającego), nie generuje certyfikatów z podpisem elektronicznym, nie prowadzi komunikacji przez SMS.

2.2.5 Wdrożenie kluczy sprzętowych U2F

- Szkolenia z obsługi kluczy realizowane w grupach do 40 osób, z instrukcjami elektronicznymi (Windows, Android).
- Szkolenie follow-up miesiąc po wydaniu wszystkich kluczy, w formie wideokonferencji z możliwością nagrania.

2.2.6 Raportowanie i ewaluacja

- Raporty generowane automatycznie z platformy po każdej kampanii, uzupełniane o komentarz ekspercki z rekomendacjami naprawczymi.
- Raporty zawierają statystyki uczestnictwa, skuteczności szablonów, liczbę użytkowników niebiorących udziału w kampanii.
- Konsultacje z zespołem ds. bezpieczeństwa po każdej kampanii (forma elastyczna).

2.2.7 Wsparcie powdrożeniowe i konsultacje

- 10 godzin konsultacji miesięcznie do wykorzystania na indywidualne konsultacje lub doradztwo (online).
- Okresowe konsultacje/przeglądy programu online.

3 Cele i mierzalne efekty programu

3.1 Cele strategiczne i operacyjne

Celem programu jest trwałe podniesienie poziomu świadomości i kompetencji pracowników Urzędu Zamówień Publicznych w zakresie cyberbezpieczeństwa, co ma przełożyć się na:

- **Zmniejszenie podatności organizacji na ataki socjotechniczne** (phishing, smishing, ataki przez komunikatory),
- **Wzrost liczby zgłoszeń podejrzanych wiadomości** i proaktywnego reagowania na zagrożenia,
- **Zwiększenie zaangażowania użytkowników** w działania edukacyjne i utrwalenie nawyków bezpiecznego zachowania,
- **Budowę kultury bezpieczeństwa** oraz trwałą zmianę postaw pracowników w zakresie ochrony informacji,
- **Zwiększenie odporności organizacji** na wycieki danych, naruszenia bezpieczeństwa systemów oraz konsekwencje prawne i wizerunkowe.

Program ma charakter ciągły i adaptacyjny, a jego celem jest nie tylko realizacja kursów, ale przede wszystkim trwała zmiana postaw i zachowań użytkowników.

3.2 Wskaźniki efektywności (KPI)

Efektywność programu będzie monitorowana na bieżąco za pomocą narzędzi analitycznych platformy szkoleniowej oraz raportów eksperckich. Główne KPI obejmują:

- **Phishing Failure Rate** – odsetek użytkowników, którzy dali się złapać na symulowany phishing (kliknięcie, podanie danych).
- **Phishing Report Rate** – odsetek użytkowników, którzy prawidłowo zgłosili podejrzaną wiadomość.
- **User Engagement** – udział użytkowników w mikro-lekcjach (procent aktywnych, liczba ukończonych lekcji, średni czas reakcji).
- **Poziom wiedzy użytkowników** – wyniki testów i quizów w kluczowych grupach tematycznych (polityki haseł, inżynieria społeczna, praca zdalna, poruszanie się po internecie, media społecznościowe, phishing, malware, bezpieczeństwo urządzenia fizycznego, ochrona danych), mierzony na bieżąco po każdej mikro-lekcji/temacie.
- **Liczba użytkowników niebiorących udziału w kampaniach** – monitorowanie i raportowanie wskaźników również dla użytkowników, którzy nie ukończyli żadnej mikro-lekcji lub nie wzięli udziału w kampanii phishingowej.

Wskaźniki będą raportowane ogólnie oraz w narzędziu szkoleniowym, z możliwością segmentacji użytkowników (wg działów, ról) w raportach i kampaniach.

3.3 Sposób pomiaru, raportowania i ewaluacji

- **Pomiar bazowy:** Przed rozpoczęciem programu wykonawca przeprowadzi testy wiedzy oraz pierwszą symulację phishingu, aby ustalić poziom wyjściowy odporności i zaangażowania.
- **Raportowanie:** Raporty generowane automatycznie z platformy szkoleniowej po każdej kampanii, uzupełniane o komentarz ekspercki (osobny dokument). Raporty zawierają prezentację wskaźników, trendów oraz rekomendacje dotyczące dalszych działań edukacyjnych (w szczególności działań naprawczych dla grup z niskim zaangażowaniem).
- **Forma raportów:** Brak wymagań co do formy graficznej; raporty mogą być w formie tabelarycznej lub graficznej, zgodnie z możliwościami platformy.
- **Archiwizacja:** Raporty i rekomendacje przekazywane zamawiającemu po każdej kampanii, bez konieczności prowadzenia archiwum przez wykonawcę.

3.4 **Konsultacje:** Po każdej kampanii wykonawca prowadzi konsultacje z zespołem ds. bezpieczeństwa zamawiającego Konsultacje i rekomendacje eksperckie

- Po każdej kampanii wykonawca przygotowuje komentarz ekspercki z rekomendacjami dotyczącymi dalszych działań edukacyjnych, skupiając się na działaniach naprawczych (np. dodatkowe szkolenia dla grup z niskim engagement).
- Rekomendacje mają formę ogólnego opisu i są konsultowane oraz zatwierdzane przez zespół ds. bezpieczeństwa zamawiającego przed wdrożeniem.
- Wykonawca prowadzi konsultacje z zespołem ds. bezpieczeństwa wyłącznie online.

4 Odbiorcy programu i podział na grupy

4.1 Odbiorcy programu

Program podnoszenia świadomości cyberbezpieczeństwa skierowany jest do wszystkich pracowników Urzędu Zamówień Publicznych, z uwzględnieniem ich zróżnicowanych ról, zakresów obowiązków oraz poziomu dostępu do informacji. Program obejmuje zarówno działania edukacyjne wspólne dla całej organizacji, jak i dedykowane ścieżki szkoleniowe dla wybranych grup funkcyjnych.

4.2 Podział na grupy funkcyjne

W ramach realizacji programu wyodrębniono następujące grupy odbiorców:

- **Kierownictwo** – 5 osób Uczestniczą w indywidualnych spotkaniach 1:1, których zakres obejmuje przekrojowe zagadnienia cyberbezpieczeństwa, analizę OSINT oraz czas na pytania indywidualne.
- **Dyrektorzy** – 17 osób Uczestniczą w indywidualnych spotkaniach 1:1, z naciskiem na praktyczne aspekty zarządzania ryzykiem, ochronę danych i komunikację w zespole.
- **Orzecznicy KIO** – 60 osób Uczestniczą w szkoleniach stacjonarnych, webinarach i mikro-lekcjach, ze szczególnym uwzględnieniem ochrony wrażliwych danych i odporności na socjotechnikę.
- **Kontrolerzy** – 40 osób Uczestniczą w szkoleniach stacjonarnych, webinarach i mikro-lekcjach, z naciskiem na bezpieczeństwo pracy z dokumentacją i nośnikami danych.

- **Pozostali pracownicy biurowi** – ok. 100 osób Uczestniczą w szkoleniach stacjonarnych, webinarach i mikro-lekcjach, z naciskiem na codzienną higienę cyfrową, ochronę danych i odporność na phishing.

4.3 Zasady podziału i uczestnictwa

- Podział na grupy jest stały przez cały okres trwania programu; nie przewiduje się zmian liczebności grup ani przypisywania pracowników do więcej niż jednej grupy.
- Nie przewiduje się wyłączeń pracowników z programu (np. z powodu nieobecności czy urlopu).
- Szkolenia indywidualne dla nowych pracowników (do 10 szkoleń w okresie umowy) realizowane są wyłącznie zdalnie, w dni robocze w godzinach pracy urzędu, na żądanie Zamawiajacego, z możliwością grupowania w przypadku kilku zgłoszeń w jednym tygodniu.
- W przypadku szkoleń grupowych dla nowych pracowników nie ma limitu liczby uczestników.
- Przewodnik po bezpieczeństwie (2 strony, elektronicznie) przekazywany jest każdemu nowemu pracownikowi.
- Komunikacja dotycząca terminów szkoleń prowadzona jest wyłącznie z uczestnikami, drogą e-mail.
- Szkolenia indywidualne/grupowe mogą być nagrywane na platformie MS Teams zamawiającego, za zgodą uczestników; wykonawca wyraża zgodę na utrwalenie wizerunku.
- Wykonawca prowadzi statystyki liczby przeprowadzonych szkoleń kwartalnie i na koniec umowy (maksymalnie 10 szkoleń w okresie umowy).

4.4 Materiały powitalne i onboarding

- Każdy nowy pracownik otrzymuje przewodnik po bezpieczeństwie w formie elektronicznej.
- Przewodnik nie wymaga aktualizacji w trakcie umowy, a jego zakres obejmuje aktualne strategie ataków cyber, sposoby rozpoznania zagrożeń oraz omówienie zasad zgłaszania incydentów obowiązujących w urzędzie.

5 Cykl szkoleniowy – program i harmonogram

5.1 Struktura cyklu szkoleniowego

Program szkoleniowy obejmuje działania edukacyjne prowadzone w kilku komplementarnych formatach, dostosowanych do specyfiki i potrzeb poszczególnych grup pracowników Urzędu Zamówień Publicznych. Cykl szkoleniowy łączy bloki wspólne dla wszystkich oraz dedykowane moduły dla grup funkcyjnych, a także szkolenia indywidualne dla nowych pracowników.

5.2 Bloki wspólne dla wszystkich pracowników

- Szkolenia stacjonarne
- Webinary (szkolenia zdalne)
- **Mikro-lekcje na platformie szkoleniowej**: Cotygodniowe, automatycznie dostarczane mikro-lekcje (2–5 minut), z powiadomieniem e-mail. Treści mogą pochodzić z biblioteki platformy lub być autorskie. Mikro-lekcje obejmują kluczowe zagadnienia: phishing, polityki haseł, inżynieria społeczna, praca zdalna, ochrona danych, bezpieczeństwo urządzeń, media społecznościowe, malware, wykorzystanie AI w dezinformacji. Szczegółowy zakres tematów zostanie określony na etapie realizacji umowy.

5.3 Moduły dedykowane grupom funkcyjnym

- **Kierownictwo (5 osób)**: Spotkania indywidualne 1:1 (stacjonarne), trwające 45–60 minut, przygotowane na podstawie OSINT, z czasem na pytania indywidualne. Zakres spotkania obejmuje przekrojowe zagadnienia, analizę indywidualnych zagrożeń, odpowiedzialność prawną i organizacyjną, zarządzanie ryzykiem oraz wdrażanie kultury bezpieczeństwa, klucze U2F.
- **Dyrektorzy (17 osób)**: Spotkania indywidualne 1:1 (stacjonarne), 45–60 minut, przygotowane na podstawie OSINT, z naciskiem na praktyczne aspekty zarządzania ryzykiem, ochronę danych i komunikację w zespole, klucze U2F.
- **Orzecznicy KIO, kontrolerzy, pracownicy biurowi**: Dedykowane bloki tematyczne w ramach szkoleń stacjonarnych, webinarów i mikro-lekcji, uwzględniające specyfikę pracy, typowe zagrożenia oraz praktyczne aspekty bezpieczeństwa.

5.4 Szkolenia indywidualne dla nowych pracowników

- Program szkolenia obejmuje aktualne strategie ataków cyber, sposoby rozpoznania zagrożeń oraz omówienie zasad zgłaszania incydentów obowiązujących w urzędzie.

- Każdy nowy pracownik otrzymuje przewodnik po bezpieczeństwie (2 strony, elektronicznie).

5.5 Tematyka szkoleń

- W całym cyklu szkoleniowym wykonawca omówi tematy: najpopularniejsze zagrożenia, phishing, socjotechnika, incydenty bezpieczeństwa, złośliwe oprogramowanie, higiena cyfrowa, bezpieczeństwo poczty elektronicznej, bezpieczeństwo urządzeń przenośnych, MFA, ślady cyfrowe, ochrona danych osobowych, praca zdalna, bezpieczeństwo nośników, OSINT, ransomware, polityka haseł, bezpieczeństwo w mediach społecznościowych, praktyczne ćwiczenia i symulacje ataków.
- Wykonawca zrealizuje 10 webinarów obejmujących swoim zakresem wszystkie powyższe tematyki, przy czym w miesiącu odbędzie się co najmniej 1 webinar.
- Co najmniej dwa webinary poświęcone zostaną wykorzystaniu platformy MS Teams i realizacji dobrych praktyk bezpieczeństwa w oparciu o mechanizmy oferowane przez te platformę.

5.6 Organizacja i komunikacja

- Wykonawca prowadzi komunikację z uczestnikami szkoleń i nowych pracowników wyłącznie drogą e-mail (potwierdzenie terminu).
- Szkolenia stacjonarne i webinary prowadzone w siedzibie zamawiającego lub na platformie MS Teams zamawiającego.
- Materiały szkoleniowe przygotowuje wykonawca dla wszystkich szkoleń.
- Nagrania webinarów i szkoleń/grupowych realizowane przez zamawiającego na platformie MS Teams.

5.7 Statystyki i raportowanie

- Wykonawca prowadzi statystyki liczby przeprowadzonych szkoleń dla nowych pracowników, raportowane kwartalnie i na koniec umowy.
- Brak wymagań dotyczących ewidencji uczestnictwa w szkoleniach stacjonarnych i webinarach.

6 Kampanie cyber awareness i symulacje ataków

6.1 Zakres kampanii i rodzaje symulacji

W ramach programu realizowane będą regularne kampanie cyber awareness, których celem jest praktyczne wzmacnianie odporności pracowników Urzędu Zamówień

Publicznych na ataki socjotechniczne oraz utrwalanie nawyków bezpiecznego zachowania. Kampanie obejmują symulacje ataków phishingowych (e-mail), smishingowych (SMS), przez komunikatory (MS Teams lub inne popularne komunikatory wykorzystywane przez pracowników) oraz podrzucenie pendrive w siedzibie Zamawiającego. Zamawiający przewiduje również realizację ataków telefonicznych (vishing) do trzech osób pełniących w Urzędzie określone funkcje. Zakres i scenariusz kampanii zostanie uzgodniony w trakcie realizacji umowy.

Każda z form ataku (e-mail, SMS, komunikatory, podrzucenie fizycznego urządzenia) zostanie wykorzystana co najmniej dwukrotnie w trakcie trwania umowy. Kampanie mogą być mieszane – w danym miesiącu może być realizowana tylko jedna z form, jednak w całym okresie obowiązywania umowy każda forma zostanie użyta zgodnie z powyższym wymogiem.

Kampanie będą targetowane zarówno na całą organizację (co najmniej 60% akcji), jak i na wybrane grupy funkcyjne (do 40% akcji, w uzgodnieniu z zamawiającym). Zamawiający wymaga realizacji usługi w dni robocze w godzinach 8:00 – 15:00 według harmonogramów opracowanych przez Wykonawcę w uzgodnieniu z Zamawiającym.

6.2 Raportowanie i analityka

Po każdej kampanii wykonawca przygotowuje raport zawierający:

- szczegółową analizę skuteczności poszczególnych szablonów ataków (np. które szablony były najskuteczniejsze),
- statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii,
- monitoring i raportowanie wskaźników również dla użytkowników, którzy nie ukończyli żadnej mikro-lekcji lub nie wzięli udziału w kampanii phishingowej,
- rekomendacje dotyczące konkretnych działań naprawczych dla grup z niskim zaangażowaniem.

Raporty będą każdorazowo konsultowane z zespołem ds. bezpieczeństwa zamawiającego po każdej kampanii (forma konsultacji elastyczna: spotkanie online, raport pisemny lub inna uzgodniona).

Szablony komunikatów do użytkowników (np. powiadomienia o wynikach kampanii) będą każdorazowo zatwierdzane przez zamawiającego przed wysyłką. Wykonawca przekazuje szablony zamawiającemu do akceptacji.

6.3 Organizacja i logistyka

- Każda kampania obejmuje ok. 200 użytkowników.

- Wykonawca prowadzi statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii (ogólna liczba, bez podziału na grupy funkcyjne).
- Wykonawca prowadzi monitoring i raportowanie wskaźników również dla użytkowników, którzy nie ukończyli żadnej mikro-lekcji lub nie wzięli udziału w kampanii phishingowej.
- Wykonawca prowadzi konsultacje z zespołem ds. bezpieczeństwa po każdej kampanii.
- Wykonawca nie prowadzi archiwum wszystkich komunikatów do użytkowników dotyczących wyników kampanii – wystarczy przekazanie szablonów zamawiającemu.

7 Platforma szkoleniowa – prowadzenie cyklu mikro-lekcji oraz mailingowych akcji phishingowych przez platformę posiadaną przez Zamawiającego

8 Platforma szkoleniowa stanowi centralny element programu edukacyjnego, zapewniając automatyzację procesu nauki, segmentację użytkowników, raportowanie i archiwizację danych oraz personalizację interfejsu zgodnie z identyfikacją wizualną zamawiającego. . Raportowanie i ewaluacja

8.1 Zakres i częstotliwość raportów

Raporty generowane są automatycznie z platformy szkoleniowej po każdej kampanii cyber awareness i symulacji ataków. Po każdej kampanii wykonawca przygotowuje również komentarz ekspercki z rekomendacjami naprawczymi, szczególnie dla grup z niskim zaangażowaniem.

8.2 Format i zawartość raportów

Raporty zawierają:

- Szczegółową analizę skuteczności poszczególnych szablonów ataków,
- Statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii,

- Monitoring i raportowanie wskaźników również dla użytkowników, którzy nie ukończyli żadnej mikro-lekcji lub nie wzięli udziału w kampanii phishingowej,
- Rekomendacje dotyczące konkretnych działań naprawczych dla grup z niskim zaangażowaniem.

Raporty są przekazywane zamawiającemu po każdej kampanii, bez konieczności prowadzenia archiwum przez wykonawcę. Forma raportów (tabelaryczna lub graficzna) jest zgodna z możliwościami platformy.

8.3 Konsultacje i rekomendacje eksperckie

Po każdej kampanii wykonawca prowadzi konsultacje z zespołem ds. bezpieczeństwa zamawiającego (forma elastyczna: spotkanie online, raport pisemny lub inna uzgodniona). Rekomendacje mają formę ogólnego opisu i są konsultowane oraz zatwierdzane przez zespół ds. bezpieczeństwa zamawiającego przed wdrożeniem.

9 Wsparcie powdrożeniowe i konsultacje

9.1 Godziny konsultacyjne i doradztwo

W ramach umowy wykonawca zapewnia 10 godzin konsultacji miesięcznie, które zamawiający może wykorzystać na indywidualne konsultacje, doradztwo lub wsparcie eksperckie (realizowane online).

9.2 Organizacja konsultacji okresowych

Przewidziane są okresowe konsultacje/przeglądy programu online, których celem jest omówienie postępów, wyników raportowania oraz rekomendacji dotyczących dalszych działań edukacyjnych.

Zasady komunikacji Wszelka komunikacja prowadzona jest drogą elektroniczną (e-mail), a w przypadku konsultacji – również w formie wideokonferencji.

10 Wymagania formalne i zgodność

10.1 Oznaczenia materiałów i dokumentów

Wszystkie materiały, dokumenty i efekty pracy muszą być oznaczone zgodnie z wymogami Księgi Identyfikacji Wizualnej KPO oraz zawierać informację o finansowaniu ze środków KPO i NextGenerationEU. Zamawiający udostępni wzory oznaczeń i logotypów.

10.2 Wymogi informacyjne i promocyjne

Wykonawca zobowiązany jest do stosowania się do wytycznych dotyczących komunikacji i promocji projektu, w tym do przygotowania materiałów komunikacyjnych do kampanii wewnętrznej.

10.3 Zasady przetwarzania i usuwania danych

Wszystkie dane osobowe muszą być przetwarzane zgodnie z RODO/GDPR. Przetwarzanie i retencja danych odbywa się wyłącznie w regionie UE/EOG. Po zakończeniu umowy wykonawca przekazuje zamawiającemu możliwość samodzielnego utrzymania platformy i nie przechowuje danych użytkowników.

10.4 Retencja i archiwizacja danych

Nie przewiduje się szczególnych wymagań dotyczących archiwizacji i retencji danych po zakończeniu projektu poza okresem przejściowym uzgodnionym w umowie.

10.5 Zasady równego traktowania wykonawców

Wszyscy wykonawcy są traktowani równo, a wymagania określone w OPZ mogą być spełnione rozwiązaniami równoważnymi pod względem funkcjonalnym i jakościowym.

10.6 Wymagania dotyczące języka i formatu materiałów

Materiały szkoleniowe, komunikaty i raporty przygotowywane są w języku polskim (na życzenie zamawiającego raporty mogą być dostępne w języku angielskim). Brak wymagań dotyczących formatu plików materiałów (np. PDF, DOCX, PPTX).