

Warszawa, dnia 16.10.2026

**Urząd Państwowej Komisji do spraw przeciwdziałania  
wykorzystaniu seksualnemu małoletnich poniżej lat 15**

ul. Twarda 18, 00-105 Warszawa NIP 5213902835

**Strona internetowa w sprawie zamówienia:** [www.bip.pkdp.gov.pl](http://www.bip.pkdp.gov.pl)

Osoba nadzorująca realizację zamówienia ze strony Zamawiającego:

Pan Rafał Łuba, [rafal.luba@pkdp.gov.pl](mailto:rafal.luba@pkdp.gov.pl)

**ZAPYTANIE OFERTOWE**

1. Urząd Państwowej Komisji w Warszawie zwraca się z zapytaniem ofertowym dotyczącym realizacji zamówienia, którego przedmiotem jest:

*Przeprowadzenie audytu konfiguracji i wykorzystania zabezpieczeń środowiska Microsoft 365 obejmującego w szczególności usługi Microsoft Entra ID, Microsoft Intune oraz Microsoft Defender w Urzędzie Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, z siedzibą w Warszawie przy ul. Twardej 18, w terminie od podpisania umowy do 10 grudnia 2026 roku.*

2. Opis przedmiotu zamówienia:

*Celem audytu jest ocena poprawności konfiguracji środowiska Microsoft 365, bezpieczeństwa tożsamości użytkowników, urządzeń i danych, skuteczności zastosowanych zabezpieczeń oraz stopnia wykorzystania funkcjonalności dostępnych w ramach posiadanych licencji, w tym Microsoft 365 E5.*

**I. Zakres audytu**

1. Licencje i zakres wykorzystania usług
  - 1) Inwentaryzacja posiadanych licencji, uruchomionych usług oraz objętych nimi użytkowników i urządzeń.
  - 2) Wskazanie funkcji bezpieczeństwa dostępnych, lecz niewdrożonych lub wykorzystywanych częściowo.
  - 3) Rozróżnienie rekomendacji możliwych do realizacji w ramach obecnych licencji od wymagających dodatkowych zakupów.
2. Microsoft Entra ID – tożsamość i dostęp
  - 1) Ocena stosowania uwierzytelniania wieloskładnikowego, metod uwierzytelniania i zasad dostępu warunkowego.
  - 2) Przegląd kont administracyjnych, uprawnień uprzywilejowanych i kont dostępu awaryjnego.
  - 3) Ocena obsługi ryzykownych logowań i przejęcia kont, stosownie do dostępnych funkcji.
  - 4) Ocena uprawnień aplikacji i zgód na dostęp do danych.
  - 5) Środowisko hybrydowe - integracja z MS AD – ocena konfiguracji synchronizacji (Microsoft Entra Connect / Cloud Sync): zakres synchronizowanych obiektów, metoda uwierzytelniania, uprawnienia konta synchronizacji. Audyt bezpieczeństwa lokalnej usługi Active Directory nie jest objęty zamówieniem.

- 6) Ocena blokowania starszych metod uwierzytelniania (legacy authentication, SMTP AUTH), zarządzania rolami uprzywilejowanymi (Privileged Identity Management), przeglądów dostępu oraz kont gości (B2B).
3. Microsoft Intune – zarządzanie urządzeniami
  - 1) Ocena kompletności objęcia urządzeń zarządzaniem.
  - 2) Przegląd polityk zgodności i konfiguracji oraz ich faktycznego zastosowania na reprezentatywnej próbie urządzeń (nie mniej niż 20 urządzeń, w tym urządzenia mobilne, jeżeli są zarządzane).
  - 3) Ocena szyfrowania dysków, przechowywania kluczy odzyskiwania, aktualizacji, zapory i uprawnień lokalnych administratorów, w tym zarządzania hasłami kont lokalnych administratorów (Windows LAPS) oraz reguł ograniczania powierzchni ataku (ASR).
  - 4) Przegląd zasad dostępu z urządzeń prywatnych i niezarządzanych oraz ochrony aplikacji mobilnych, jeżeli są wykorzystywane.
  - 5) Weryfikacja powiązania stanu zgodności urządzenia z zasadami dostępu do zasobów urzędu.
4. Microsoft Defender – ochrona i wykrywanie zagrożeń
  - 1) Ocena konfiguracji i pokrycia urządzeń ochroną Microsoft Defender for Endpoint, jeżeli jest wykorzystywany.
  - 2) Przegląd zabezpieczeń poczty przed phishingiem, złośliwymi załącznikami i odnośnikami.
  - 3) Ocena konfiguracji alertów, obsługi incydentów, powiadomień i odpowiedzialności administratorów.
  - 4) Weryfikacja integracji dostępnych usług Defender oraz wykorzystania funkcji ochrony tożsamości i aplikacji chmurowych, stosownie do licencji i architektury środowiska.
  - 5) Analiza wykrytych podatności, wyjątków od polityk i zaleceń bezpieczeństwa.
  - 6) Przegląd zabezpieczeń domen pocztowych (SPF, DKIM, DMARC) oraz reguł automatycznego przekazywania poczty na adresy zewnętrzne.
5. Ochrona danych w Microsoft 365
  - 1) Techniczny przegląd zasad udostępniania danych na zewnątrz w SharePoint, OneDrive i Teams.
  - 2) Ocena konfiguracji etykiet poufności i zapobiegania utracie danych (DLP), jeżeli są dostępne.
  - 3) Przegląd konfiguracji rejestrowania zdarzeń i retencji w uzgodnionym zakresie.

## **II. Sposób realizacji**

1. Wykonawca w terminie 7 dni od zawarcia umowy przedstawi Zamawiającemu do uzgodnienia plan i harmonogram realizacji audytu.
2. Audyt zostanie przeprowadzony poprzez:
  - 1) analizę konfiguracji środowiska Microsoft 365,
  - 2) wywiady z administratorami,
  - 3) przeprowadzenie uzgodnionych testów potwierdzających działanie wybranych zabezpieczeń.

Sam eksport ustawień lub raport Microsoft Secure Score nie będzie wystarczającym rezultatem. Punktem odniesienia oceny będą w szczególności aktualne wersje CIS Microsoft 365 Foundations Benchmark oraz bazowe konfiguracje zabezpieczeń (security baselines) Microsoft, z uwzględnieniem specyfiki Zamawiającego.

Dostęp Wykonawcy do środowiska odbywa się wyłącznie z kont imiennych utworzonych przez Zamawiającego, z uwierzytelnianiem wieloskładnikowym i rolami tylko do odczytu (w szczególności Global Reader, Security Reader), przydzielanymi na czas określony. Testy przeprowadza się wyłącznie po pisemnej akceptacji scenariusza przez Zamawiającego, na uzgodnionych kontaktach i urządzeniach. Testy penetracyjne i symulacje ataków socjotechnicznych nie są objęte zamówieniem, chyba że Strony postanowią inaczej.

3. Środowisko Zamawiającego obejmuje około:

- 1) 75 użytkowników,
- 2) 200 urzędzeń.
4. Audyt może być realizowany w formule stacjonarnej, zdalnej lub mieszanej, przy zapewnieniu bezpieczeństwa informacji oraz poufności przekazywanych danych.

Przed rozpoczęciem realizacji zamówienia Wykonawca będzie zobowiązany do zawarcia z Zamawiającym umowy powierzenia przetwarzania danych osobowych stanowiący załącznik nr 5 do zapytania ofertowego.

### **III. Oczekiwane rezultaty**

1. **Wykonawca przekaze raport końcowy zawierający w szczególności:**
  - 1) Ustalenia audytowe wraz z materiałem dowodowym;
  - 2) Ocenę ryzyk i ograniczenia audytu;
  - 3) Zestawienie zabezpieczeń:
    - a) wdrożonych prawidłowo,
    - b) wymagających poprawy,
    - c) niewdrożonych,
    - d) nieadekwatnych do środowiska;
  - 4) Konkretne rekomendacje konfiguracji wraz z przewidywanym wpływem na pracę użytkowników;
  - 5) Plan działań naprawczych na 30, 60 i 90 dni, z priorytetami, szacowanym nakładem pracy i zależnościami licencyjnymi;
  - 6) Podsumowanie wyników audytu;
  - 7) Wyniki uzgodnionych testów, w szczególności dotyczących wymuszania uwierzytelniania wieloskładnikowego, ograniczania dostępu z urzędzeń niespełniających wymagań oraz generowania i obsługi wybranych alertów bezpieczeństwa.

### **IV. Warsztat dla administratorów**

1. W ramach realizacji zamówienia Wykonawca przeprowadzi warsztat dla administratorów środowiska Microsoft 365 omawiający wyniki i sposób realizacji zaleceń.
2. Warsztat:
  - 1) stanowi odrębny element realizacji zamówienia,
  - 2) nie jest częścią prezentacji wyników audytu,
  - 3) powinien trwać minimum 2 godziny,
  - 4) powinien zostać przeprowadzony dla 3 administratorów,
  - 5) powinien obejmować omówienie ustaleń audytu oraz sposobu realizacji rekomendacji,
  - 6) powinien zostać przeprowadzony po przekazaniu projektu raportu, w terminie uzgodnionym w harmonogramie, nie później niż do 10 grudnia 2026 r., w formie stacjonarnej lub zdalnej.

### **V. Warunki odbioru**

1. Odbiór usługi nastąpi po przekazaniu raportu końcowego w wersji PDF oraz wersji edytowalnej.
  2. Wykonawca przekaze Zamawiającemu projekt raportu nie później niż do 26 listopada 2026 r. Zamawiający może zgłosić uwagi faktograficzne w terminie 2 dni roboczych; Wykonawca rozpatrzy je przed przekazaniem raportu końcowego.
  3. Raport powinien zawierać wszystkie elementy określone w opisie przedmiotu zamówienia.
  4. Warunkiem odbioru będzie również przeprowadzenie warsztatu dla administratorów.
3. Warunki udziału w postępowaniu oraz oświadczenia i dokumenty potwierdzające ich spełnienie:

**O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:**

1. W okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał należycie co najmniej 2 usługi, z których każda obejmowała co najmniej jeden z następujących obszarów:
  - 1) audyt bezpieczeństwa środowiska Microsoft 365,
  - 2) audyt Microsoft Entra ID,
  - 3) audyt Microsoft Intune,
  - 4) audyt Microsoft Defender,
  - 5) audyt bezpieczeństwa usług chmurowych Microsoft (Microsoft 365 lub Azure),
  - 6) lub usług o porównywalnym zakresie.
2. Wykonawca skieruje do realizacji zamówienia co najmniej jedną osobę posiadającą łącznie:
  - 1) minimum 3-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa lub administracji środowiskiem Microsoft 365, oraz
  - 2) doświadczenie w realizacji co najmniej 2 audytów bezpieczeństwa środowisk Microsoft 365 lub usług o porównywalnym zakresie.

**Wymagane dokumenty od Wykonawcy:**

1. Formularz ofertowy,
  2. Wykaz usług,
  3. Wykaz osoby przewidzianej do realizacji audytu Microsoft 365 wraz z opisem doświadczenia,
  4. Dokumenty potwierdzające należyte wykonanie usług (np. referencje, protokoły odbioru, rekomendacje).
4. Termin realizacji zamówienia: **Zamawiający wymaga, aby zamówienie było zrealizowane od daty zawarcia umowy do 10.12.2026 roku.**
  5. Termin związania ofertą:  
Wykonawca jest związany ofertą przez 30 dni od upływu terminu składania ofert.  
Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, na oznaczony okres.
  6. Miejsce i termin złożenia oferty:  
Na adres email: [rafal.luba@pkdp.gov.pl](mailto:rafal.luba@pkdp.gov.pl) w terminie do dnia 23.10.2026 , do godziny 11:00.
  7. Termin otwarcia ofert nastąpi w dniu: 23.10.2026 o godzinie 11:30.
  8. Kryteria oceny ofert i sposób oceny ofert.
    - 1) Zamawiający dokona oceny ważnych ofert na podstawie następujących kryteriów:

**I. Cena 60 pkt** – Zaproponowana przez Wykonawcę cena musi uwzględniać wszystkie koszty rzeczowe i osobowe realizacji zamówienia wynikające z niniejszego ogłoszenia i nie podlega waloryzacji w okresie obowiązywania umowy w sprawie zamówienia.

**Zamawiający będzie przyznawał punktację w następujący sposób:**

Maksymalna liczba punktów: **60 pkt** - (Cn) obliczone, według następującego wzoru:

$$Cn = \frac{C \text{ of. n.}}{C \text{ of. b.}} \times 60 \text{ (waga kryterium)}$$

gdzie:

**Cn** – liczba punktów za kryterium cena

**C of. n.** – cena oferty najniższej

**C of. b.** – cena oferty badanej

## **II. Doświadczenie osoby przewidzianej do realizacji audytu – 40 pkt**

Ocenie podlega doświadczenie osoby wskazanej przez Wykonawcę do realizacji zamówienia, wykazane w Załączniku nr 3 – Wykaz osoby przewidzianej do realizacji audytu.

Za doświadczenie uznaje się udział w realizacji audytów obejmujących:

bezpieczeństwo środowiska Microsoft 365, Microsoft Entra ID, Microsoft Intune, Microsoft Defender, bezpieczeństwo usług chmurowych Microsoft, zarządzanie tożsamością i dostępem, usługi o porównywalnym zakresie.

**Maksymalna liczba punktów: 40 pkt**

| <b>Liczba usług</b> | <b>Punkty</b> |
|---------------------|---------------|
| 2 usługi            | 0 pkt         |
| 3 usługi            | 10 pkt        |
| 4 usługi            | 20 pkt        |
| 5 usług             | 30 pkt        |
| 6 i więcej usług    | 40 pkt        |

Do oceny zostaną przyjęte wyłącznie audyty wykazane w Załączniku nr 3 – Wykaz osoby przewidzianej do realizacji audytu zawierającym dla każdego audytu: nazwę odbiorcy, okres realizacji, przedmiot i zakres audytu oraz rolę osoby w audycie. Wykaz w zakresie kryterium nie podlega uzupełnieniu ani zmianie po upływie terminu składania ofert; audyty niewykazane lub bez wymaganych danych nie są punktowane.

## **III. Łączna maksymalna liczba punktów: 100 pkt.**

- 2) W toku badania i oceny ofert Zamawiający może żądać od oferentów wyjaśnień dotyczących treści złożonych ofert, w tym wyjaśnień dotyczących rażąco niskiej ceny oraz wezwać oferentów do uzupełnienia niekompletnych ofert, a w przypadku, ich nieuzupełnienia w wyznaczonym terminie, ma prawo ofertę odrzucić.
9. Sposób przygotowania oferty:
  - a) Ofertę należy sporządzić w postaci elektronicznej, w języku polskim.
  - b) Oferta powinna zostać przesłana za pośrednictwem poczty elektronicznej.
  - c) Ofertę należy sporządzić zgodnie z [Zal\\_1 Formularz ofertowy](#) do zapytania ofertowego
  - d) Oferta powinna być podpisana przez osobę właściwie umocowaną do reprezentacji Wykonawcy. Ofertę podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym albo przesyła się skan oferty podpisanej własnoręcznie.
10. Zamawiający zastrzega sobie możliwość dokonania zmian lub odwołania warunków zawartych w niniejszym Zapytaniu ofertowym. W przypadku wprowadzenia zmian, Zamawiający przekaze informację o zmianach wszystkim Oferentom zaproszonym do złożenia oferty. Każda zmiana staje się wiążąca od chwili przekazania informacji o jej dokonaniu. W przypadku, gdy cena najkorzystniejszej oferty przekroczy możliwości finansowe Zamawiającego, postępowanie może zostać unieważnione.
11. Zamawiający może odstąpić od zawarcia umowy/udzielenia zamówienia, w każdym czasie bez podania przyczyn lub zamknąć postępowanie o udzielenie zamówienia publicznego. Oferentom nie przysługują żadne roszczenia z tytułu zamknięcia postępowania. W przypadku, gdy złożone oferty przekraczają kwotę przeznaczoną na realizację, Zamawiający zastrzega sobie prawo do przeprowadzenia negocjacji z Wykonawcami, którzy przystąpili do postępowania.
12. Zamawiający dopuszcza możliwość negocjacji ceny z wykonawcami, którzy złożyli oferty niepodlegające odrzuceniu, w przypadku, o którym mowa w pkt 11.

13. Klauzula informacyjna dotycząca przetwarzania danych osobowych.

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Urząd Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 w Warszawie, ul. Twarda 18, 00-105 Warszawa.
- 2) Kontakt z Inspektorem Ochrony Danych – [iod@pkdp.gov.pl](mailto:iod@pkdp.gov.pl).
- 3) Pani/Pana dane osobowe przetwarzane będą w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia i realizacji umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywającego na Urzędzie Państwowej Komisji jako jednostce sektora finansów publicznych (art. 6 ust. 1 lit. c RODO), a w zakresie zawarcia i realizacji umowy – art. 6 ust. 1 lit. b RODO.
- 4) Pani/Pana dane osobowe będą przetwarzane przez okres prowadzenia postępowania o udzielenie zamówienia publicznego, zawarcia i realizacji umowy oraz po jego zakończeniu zgodnie z przepisami dotyczącymi archiwizacji.
- 5) Przetwarzane dane osobowe obejmują w szczególności imię i nazwisko, adres, NIP, REGON, numer CEIDG, numer KRS oraz inne dane osobowe podane przez osobę składającą ofertę i inną korespondencję wpływającą do UPKDP w celu udziału w postępowaniu.
- 6) Odbiorcami Pani/Pana danych osobowych mogą być organy publiczne i urzędy państwowe lub inne podmioty upoważnione na podstawie przepisów prawa lub wykonujące zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej, w szczególności podmioty prowadzące działalność kontrolną wobec Urzędu Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 w Warszawie.
- 7) W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
- 8) Posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych<sup>1</sup>;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO<sup>2</sup>;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) Nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,

---

<sup>1</sup> Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego.

<sup>2</sup> Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- prawo sprzeciwu, o którym mowa w art. 21 RODO, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.

10) Jednocześnie przypominamy o ciąży na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

11) W celu potwierdzenia wypełnienia przez Wykonawcę obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO Wykonawca złoży stosowne oświadczenie. Oświadczenie zawarte jest we wzorze formularza ofertowego.

**Załączniki:**

1. *Formularz Ofertowy,*
2. *Wykaz usług,*
3. *Wykaz osoby przewidzianej do realizacji audytu Microsoft 365 wraz z opisem doświadczenia,*
4. *Projektowane postanowienia umowy (wzór umowy),*
5. *Wzór umowy powierzenia przetwarzania danych osobowych.*