

BA.V.260.27.2025

## Załącznik nr 1 do SWZ

## Opis przedmiotu zamówienia –

usługa dostępu do platformy do zarządzania tożsamością OKTA w modelu chmurowym (SaaS),  
utrzymania platformy oraz wsparcia technicznego

## Rozdział I

## Przedmiot zamówienia

- Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego usług dostępu, do platformy do zarządzania tożsamością OKTA (dalej „Platforma”) w modelu chmurowym (SaaS), utrzymania Platformy oraz wsparcia technicznego (dalej „Usługi”) w zakresie:
  1. aktualnie użytkowanych przez Zamawiającego modułów w dotychczasowym kształcie, zapewniając ciągłość i nieprzerwane funkcjonowanie Platformy w obecnej konfiguracji, udostępnionej pod adresem mapgov.okta.com, w tym:
    - 1.1. Moduł Single Sign-On (SSO)**
      - 1.1.1. utrzymanie i konfiguracja aplikacji SSO (federacje SAML 2.0, OIDC, WS-Fed),
      - 1.1.2. konfiguracja zasad logowania (adaptive authentication, MFA policies),
      - 1.1.3. zarządzanie dostępami do aplikacji zintegrowanych z OKTA,
      - 1.1.4. obsługa i weryfikacja integracji nowych aplikacji,
      - 1.1.5. wsparcie w zakresie logowań użytkowników i sesji,
    - 1.2. Moduł Universal Directory**
      - 1.2.1. wymagany jest elastyczny, oparty na chmurze katalog,
      - 1.2.2. możliwość nieograniczonej integracji z katalogami: Wsparcie dla Active Directory, LDAP i aplikacji,
      - 1.2.3. nieograniczona liczba niestandardowych atrybutów i pól użytkownika,
      - 1.2.4. możliwość mapowania i transformacji atrybutów,
      - 1.2.5. umożliwia korzystanie z protokołu LDAP bez konieczności utrzymywania lokalnej infrastruktury,
      - 1.2.6. zapewnienie zgodności z politykami bezpieczeństwa Zamawiającego,
    - 1.3. Moduł Lifecycle Management**
      - 1.3.1. utrzymanie procesów provisioningowych i deprovisioningowych,
      - 1.3.2. automatyzacja procesów przydzielania i odbierania uprawnień,
      - 1.3.3. utrzymanie integracji z aplikacjami SaaS i systemami lokalnymi,
      - 1.3.4. wsparcie dla zarządzania cyklem życia kont pracowników i współpracowników,
      - 1.3.5. monitorowanie i raportowanie przebiegu procesów LCM;
  2. dodatkowych modułów:
    - 2.1 Moduł Device Access**
      - 2.1.1. weryfikuje użytkownika przed przyznaniem dostępu,
      - 2.1.2. umożliwia definiowanie zasad bezpieczeństwa dla konkretnych urządzeń,
      - 2.1.3. zapewnia kontrolę zgodności urządzeń z polityką bezpieczeństwa organizacji,
    - 2.2. Moduł Light Workforce Identity Workflows dla minimum 50 procesów**
      - 2.2.1. obsługuje co najmniej 50 procesów (np. onboarding, offboarding, zmiany ról i uprawnień),
      - 2.2.2. umożliwia tworzenie przepływów pracy w prosty sposób bez kodowania,
      - 2.2.3. integruje się z innymi systemami w organizacji, przyspieszając i ułatwiając operacje administracyjne,
    - 2.3. Moduł Adaptive MFA**
      - 2.3.1. dostosowuje poziom uwierzytelnienia do kontekstu logowania (lokalizacja, urządzenie, ryzyko),
      - 2.3.2. wspiera wiele metod MFA (push, SMS, tokeny, biometryka),
      - 2.3.3. zapewnia wyższy poziom bezpieczeństwa bez obniżania wygody użytkownika,

## 2.4. Moduł Identity Threat Protection

- 2.4.1. monitoruje logowania, zachowania i anomalie w dostępie użytkowników,
- 2.4.2. wykrywa podejrzane aktywności (np. kradzież konta, nietypowe logowania),
- 2.4.3. automatycznie podejmuje działania prewencyjne, np. blokuje dostęp lub wymusza MFA.

- W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest zapewnić dostęp do Platformy dla minimum 400 użytkowników.
- Wykonawca będzie zobowiązany do rozpoczęcia świadczenia Usług przez okres 12 miesięcy liczony od dnia potwierdzenia odbioru nie wcześniej niż od dnia 18 grudnia 2025 r.
- Wykonawca zapewni zgodność świadczenia Usług oraz opracowanych dokumentów z obowiązującymi przepisami prawa, w szczególności z:
  1. rozporządzeniem 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 – dalej również: „RODO”) <sup>1</sup>. Wykonawca zobowiązany jest – w celu potwierdzenia spełnienia wymogów dotyczących ochrony danych osobowych - wypełnić raport sporządzony wg wzoru stanowiącego załącznik nr 1 do OPZ „Opis środków technicznych i organizacyjnych wprowadzonych przez Wykonawcę” i przekazać go wraz z ofertą. W związku z realizacją Umowy, w zakresie w jakim jej wykonanie wiąże się z przetwarzaniem danych osobowych, Wykonawca zawrze z Zamawiającym odrębną Umowę powierzenia przetwarzania danych osobowych, zgodnie z art. 28 RODO wg wzoru stanowiącego załącznik do umowy.  
Wykonawca zobowiązany jest realizować zamówienie zgodnie z obowiązującymi przepisami, w szczególności z:
    1. ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
    2. ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne<sup>2</sup>,
    3. ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych<sup>3</sup>,
    4. ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa<sup>4</sup>.

## Rozdział II

### 1. Warunki wsparcia technicznego i utrzymania

#### 1.1. Definicje

- Godziny pracy – dni robocze, od poniedziałku do piątku, w godzinach od 8:00 do 17:00 z pominięciem dni ustawowo wolnych od pracy.
- Przyjęcie zgłoszenia – mailowe potwierdzenie przez pracownika działu wsparcia Wykonawcy lub przez system rejestracji zgłoszeń zarejestrowania zgłoszenia.
- Czas rozwiązania – czas, w jakim Wykonawca usunie na Platformie zgłoszony incydent lub - w przypadku gdy zgłoszenie nie dotyczy działania Platformy - dostarczy użytkownikowi rozwiązania.

#### 1.2. Zakres wsparcia technicznego i utrzymania

Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego i utrzymania obejmującego :

- obsługę: telefoniczną, za pomocą poczty elektronicznej oraz systemów zdalnej pomocy,
- dostęp online do dokumentacji technicznej oraz poprawek do Platformy.

Wsparcie techniczne i utrzymanie obejmuje:

- a) pomoc techniczną producenta Platformy;

<sup>1</sup> Dz.Urz.UE.L Nr 119, str. 1.

<sup>2</sup> Dz.U. z 2024 r. poz. 307.

<sup>3</sup> Dz.U. z 2023 r. poz. 1270

<sup>4</sup> Dz.U. z 2023 r. poz. 913

- b) dostęp do poprawek i nowych wersji Platformy;
- c) zapewnienie zdalnej pomocy technicznej (telefoniczne, mailowe i online ) w języku polskim w Godzinach Pracy;
- d) obsługę zgłoszeń typu „How to”.

Wykonawca gwarantuje, że przez co najmniej 98,5% czasu świadczenia Usługi (12 miesięcy) oraz nie mniej niż 98,5% w ciągu każdego miesiąca kalendarzowego System będzie działał prawidłowo, to znaczy umożliwi zarówno bezawaryjne, jak i zgodne z OPZ użytkowanie.

### **1.3. Klasyfikacja zgłoszeń**

Wykonawca zobowiązany jest do klasyfikacji zgłoszeń Zamawiającego oraz i nadawania im priorytetów obsługi zgodnie z następującymi warunkami:

- Incydent o dotkliwości S1- powstaje, gdy Platforma nie jest w stanie właściwie funkcjonować zgodnie z opisem funkcjonalności zawartym w dokumentacji technicznej, a sytuacja ta wpływa w sposób niekorzystny na działalność Zamawiającego w całości.
- Incydent o dotkliwości S2 - powstaje, gdy Platforma nie jest w stanie właściwie funkcjonować, zgodnie z opisem funkcjonalności zawartej w dokumentacji, a sytuacja ta wpływa w sposób niekorzystny na działalność Zamawiającego i jednocześnie Platforma częściowo działa.
- Incydent o dotkliwości S3 – powstaje, gdy Platforma nie jest w stanie właściwie funkcjonować, zgodnie z opisem funkcjonalności zawartej w dokumentacji, a sytuacja ta nie wpływa w istotny sposób na działalność Zamawiającego.
- Incydent o dotkliwości S4 - to drobne usterki i problemy mające znikomy wpływ na funkcjonowanie Platformy.

### **1.4. Czasy reakcji i przewidywane czasy rozwiązania zgłoszeń**

Wykonawca zobowiązany jest do zapewnienia terminowego rozwiązywania zgłoszeń Zamawiającego

w oparciu o przyjęte czasy reakcji i przewidywane czasy rozwiązania dla sklasyfikowanych zgłoszeń:

- Incydent o dotkliwości S1 – przyjęcie zgłoszenia w ciągu 30 minut w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia 2 dni w Godzinach Pracy.
- Incydent o dotkliwości S2 – przyjęcie zgłoszenia w ciągu 4 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia do 4 dni w Godzinach Pracy.
- Incydent o dotkliwości S3 – przyjęcie zgłoszenia w ciągu 8 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia w ciągu 10 dni w Godzinach Pracy.
- Incydent o dotkliwości S4 – przyjęcie zgłoszenia w ciągu 12 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia przy następnej aktualizacji producenta.

### **1.5. Sposób dostępu do Platformy**

W ramach kontynuacji świadczenia Usług Zamawiający wymaga utrzymania portalu mapgov.okta.com z jej pełną konfiguracją.

### **2. Wymagania techniczne dostępu do Platformy**

- Wspierane systemy operacyjne: Windows 10 / 11, macOS (najnowsze wersje).
- Wspierane przeglądarki: Google Chrome (ostatnie 2 wersje), Microsoft Edge (Chromium), Mozilla Firefox (ostatnie 2 wersje), Apple Safari (na macOS i iOS).
- Aplikacja mobilna (dla MFA) Okta Verify dostępna w: Google Play (Android 8.0 lub nowszy), App Store (iOS 15 lub nowszy).
- Wymaga połączenia z Internetem (Wi-Fi lub dane mobilne) aparatu (do zeskanowania kodu QR przy pierwszej konfiguracji).

## **Rozdział III**

**Główny kod CPV:** 72222300-0 – Usługi w zakresie technologii informacji, 72253100-0 – Usługi w zakresie utrzymania oprogramowania, 72212732-9 – Oprogramowanie do zarządzania tożsamością użytkownika, 72267000-4 – Usługi w zakresie konserwacji i wsparcia oprogramowania.

Załącznik nr 1

do opisu przedmiotu zamówienia: Opis technicznych i organizacyjnych środków ochrony danych osobowych wprowadzonych przez Wykonawcę – **zestawienie środków w wersji edytowalnej do załączenia do oferty stanowi Załącznik nr 5 do SWZ.**

L.p.	TAK/NIE	W przypadku braku zabezpieczenia należy uzasadnić	Wdrożone środki bezpieczeństwa
<b>I. Środki ochrony fizycznej</b>			
			Serwery zlokalizowane są na terytorium Europejskiego Obszaru Gospodarczego.
			Serwery zlokalizowane są w pomieszczeniach z dostępem wyłącznie dla osób posiadających nadane uprawnienia (System Kontroli Dostępu – SKD, System Zarządzania Kluczami - SZK).
			Służba ochrony prowadzi całodobową, fizyczną ochronę budynku.
			Hol główny i teren wokół budynku jest objęty monitoringiem wizyjnym (CCTV).
			Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami zwykłymi (nie wzmacnianymi, nie przeciwpożarowymi).
			Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej.
			Dane osobowe Zamawiającego są przechowywane w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie.
			Dane osobowe Zamawiającego (w tym dane są przechowywane w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
			Pomieszczenia wyposażone są w system alarmowy przeciwwłamaniowy (SSWiN).
			Dostęp do pomieszczeń objęty jest systemem kontroli dostępu (SKD).
			Dostęp do pomieszczeń objęty jest zasadami zarządzania dostępem do kluczy do pomieszczeń (np. system zarządzania kluczami, depozytory - SZK)
			Dostęp do pomieszczeń kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych (CCTV).
			Dostęp do pomieszczeń w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
			Pomieszczenia są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy.
			Kopie zapasowe przechowywane są w różnych lokalizacjach, na różnych nośnikach.
<b>II. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej</b>			

			Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny przed skutkami awarii zasilania.
			Każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych.
			Dostęp do zasobów Zamawiającego zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
			System informatyczny zapewnia wymuszenie na użytkowniku okresową zmianę hasła.
			System informatyczny zapewnia zmianę hasła w razie zaistniałej potrzeby.
			Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii przy użyciu systemów informatycznych.
			Zastosowano system rejestracji dostępu do systemu.
			Zastosowano środki kryptograficznej ochrony danych przekazywanych drogą teletransmisji.
			Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
			Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity. (oprogramowanie antywirusowe).
			Oprogramowanie posiada licencje i jest na bieżąco aktualizowane.
			Użyto system Firewall do ochrony dostępu do sieci komputerowej.
			Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
			Zapewniono zdolność do szybkiego przywrócenia dostępności informacji i dostępu do nich w razie incydentu fizycznego i technicznego.
			Dostęp do danych osobowych Zamawiającego zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

### III. Środki ochrony w ramach narzędzi programowych i baz danych

			Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach danych.
			Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych informacji.
			Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
			Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
			Dostęp do zasobów Zamawiającego wymaga logowania/uwierzytelnienia poprzez uwierzytelnianie wielopoziomowe, np. 2FA (uwierzytelnianie dwuskładnikowe).
			Dostęp do zasobów Zamawiającego wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.

			Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego.
			Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zasobów Zamawiającego.
			Zastosowano kryptograficzne środki ochrony danych.
			Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe Zamawiającego.
			Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania informacji Zamawiającego ( w tym danych osobowych) w przypadku dłuższej nieaktywności pracy użytkownika.
<b>IV. Środki organizacyjne</b>			
			Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
			Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
			Cyklicznie doskonalona jest wiedza osób zatrudnionych przy przetwarzaniu informacji poprzez cykliczne szkolenia oraz inne działania podnoszące świadomość w przedmiotowym obszarze.
			Wprowadzono/określono zasady ochrony danych osobowych przetwarzanych w systemach teleinformatycznych.
			Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
			Dostęp do pomieszczeń po godzinach pracy nie jest możliwy dla osób trzecich (np. firmy sprzątającej) bądź dostęp ten jest szczegółowo nadzorowany.
			Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
			Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób – zgodnie z polityką czystego ekranu.
			Określono zakres oraz częstotliwość tworzenia kopii zapasowych.
			Określono procedury odtwarzania systemu po awarii oraz ich testowania.
			Przeprowadzono szacowanie ryzyka dla aktywów w których będą przetwarzane będą dane osobowe Zamawiającego.
			Wdrożenie wymogów dotyczących bezpieczeństwa informacji potwierdzone jest stosownymi certyfikatami.
			Wdrażanie nowych rozwiązań odbywa się zgodnie z zasadą „privacy by design”.
			Wdrażanie nowych rozwiązań odbywa się zgodnie z zasadą z zasadą „privacy by default”.
			Prowadzona jest ocena skutków dla ochrony danych.
			Gwarantowana jest realizacja praw osób, których dane dotyczą.

			Gwarantowane jest przestrzeganie procedury informowania Administratora o naruszeniu ochrony danych osobowych.
			Prowadzony jest monitoring funkcjonującego systemu ochrony danych osobowych.
			Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
			Do przetwarzania danych osobowych dopuszczone są jedynie osoby posiadające upoważnienie do przetwarzania danych osobowych.
			Wdrożona i stosowana jest polityka określająca zasady ochrony danych osobowych.