



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo
Rozwoju i Technologii

Ministerstwo Rozwoju i Technologii
ul. Plac Trzech Krzyży 3/5
00-507 Warszawa

Warszawa, 24 maja 2024 r.

OPIS PRZEDMIOTU ZAMÓWIENIA

dotyczącego zakupu usługi hostingu i administrowania, wraz z zapewnieniem wysokiej sprawności i szybkości przetwarzania danych, narzędziem SmartRadar Ministerstwa Rozwoju i Technologii

I. ZAMAWIAJĄCY

Ministerstwo Rozwoju i Technologii
ul. Plac Trzech Krzyży 3/5
00-507 Warszawa

II. POSTANOWIENIA OGÓLNE

1. Ministerstwo Rozwoju i Technologii, Departament Innowacji i Polityki Przemysłowej, z siedzibą przy Pl. Trzech Krzyży 3/5, 00-507 Warszawa, zaprasza do składania ofert w ramach zapytania ofertowego dot. zakupu usługi hostingu i administrowania, wraz z zapewnieniem wysokiej sprawności i szybkości przetwarzania danych, narzędziem SmartRadar Ministerstwa Rozwoju i Technologii
2. Osobą uprawnioną do kontaktów roboczych w ramach niniejszego zamówienia ze strony zamawiającego jest Wiesław Śmierzyński tel. (22) 411-93-91, email: wieslaw.smierzynski@mrit.gov.pl
3. Zamówienie jest współfinansowane ze środków Funduszy Europejskich dla Nowoczesnej Gospodarki oraz środków budżetowych.

III. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest świadczenie usługi związanej z zapewnieniem hostingu i administrowaniem narzędziem interaktywnym smartradar.smart.gov.pl, którego właścicielem jest Ministerstwo Rozwoju i Technologii. SmartRadar znajduje się na domenie smart.gov.pl poświęconej krajowym inteligentnym specjalizacjom – obszarom technologicznym o największym potencjale rozwojowym, na których koncentruje się wsparcie w ramach programów finansowanych ze środków UE z przeznaczeniem na wsparcie innowacyjności.

Narzędzie SmartRadar służy do monitoringu inteligentnych specjalizacji na poziomie krajowym i regionalnym. Umożliwia ono gromadzenie, przetwarzanie i prezentację danych na portalu internetowym w zakresie innowacyjności gospodarki oraz poszczególnych branż i obszarów określonych jako inteligentne specjalizacje. Odbiorcami treści portalu SmartRadar są osoby zainteresowane polityką innowacyjności, polityką technologiczną, monitorowaniem inteligentnych specjalizacji na poziomie krajowym i regionalnym, instrumentami wsparcia prac badawczo-rozwojowych i innowacyjnych projektów, w tym w ramach programów operacyjnych finansowanych ze środków UE tj. przedsiębiorcy, przedstawiciele administracji publicznej, jednostki naukowe, przedstawiciele instytucji otoczenia biznesu, NGOs, obywatele.

IV. TERMIN REALIZACJI ZAMÓWIENIA

Termin realizacji usługi hostingu i administrowania narzędzia interaktywnego SmartRadar – w okresie od podpisania umowy do dnia 31.12.2024r.

V. WYMAGANIA DOTYCZĄCE REALIZACJI ZAMÓWIENIA

1. Wykonawca zapewni przestrzeń serwerową na własnych zasobach (dedykowany serwer/serwery, łącze internetowe) i będzie świadczył usługi hostingu oraz administrowania dla narzędzia interaktywnego SmartRadar Ministerstwa Rozwoju i Technologii przez okres 6 miesięcy od dnia podpisania umowy.
2. W ramach usług zostanie zapewnione prawidłowe i bezawaryjne działanie narzędzia SmartRadar oraz monitorowanie stanu działania oraz wydajność narzędzia SmartRadar.
3. W ramach usługi hostingu i administrowania narzędziem SmartRadar Wykonawca zgodnie z obowiązującymi standardami technicznymi, zapewni:
 - 1) poprawne wczytywanie oraz wyświetlanie stron, usuwanie błędów funkcjonowania;
 - 2) aktualizacje treści komunikatów narzędzia SmartRadar, takie jak zmiana tekstu w opisach poszczególnych zakładek, napisów w dymkach objaśniających, w słowniku bazy danych czy też podmiana slajdów na stronie głównej;
 - 3) poprawne funkcjonowanie linków do innych stron, danych, plików narzędzia SmartRadar;
 - 4) przestrzeganie standardów bezpieczeństwa w tym obsługę uprawnień dla użytkowników wewnętrznych narzędzia SmartRadar;
 - 5) zgodność portalu z wytycznymi WCAG 2.1;
 - 6) poprawny import danych dla wskaźników i projektów programów operacyjnych z plików excel wg szablonów oraz poprzez import za pomocą API w aplikacji SmartRadar, w tym implementacja zmian w linkach API;
 - 7) funkcjonowanie narzędzia SmartRadar podczas aktualizacji bazy danych przez osoby uprawnione do logowania do panelu administracyjnego narzędzia ze strony Zamawiającego w oparciu o nowe dane lub metadane (przez łącza API oraz pliki Excel);
 - 8) instalacje najnowszych wersji i aktualizacji narzędzi wykorzystanych w usłudze hostingu i administrowania portalami Zamawiającego (m.in.: wgranie wersji oraz poprawek łatających luki w zabezpieczeniach, kontrolę poprawności działania po wgraniu nowej wersji/poprawki, usunięcie ewentualnych błędów oraz niezgodności po wgraniu nowej wersji/poprawki, kontrola stabilności portalu po zmianach);
 - 9) instalację oraz aktualizację elementów narzędzia SmartRadar. Każdorazowo instalacja bądź aktualizacja obejmować będzie czynności polegające na zatrzymaniu serwera aplikacyjnego, wymianie (wgraniu) zbudowanej wersji narzędzia oraz na wznowieniu pracy serwera aplikacyjnego. Czynności te zawsze będą wykonywane w wyznaczonym oknie serwisowym bądź ustalonym terminie. Każdorazowe wgranie nowej wersji systemu zakończone zostanie weryfikacją poprawności działania serwera aplikacyjnego;
 - 10) instalację, konfigurację narzędzi pozwalających śledzić wydajność SmartRadar, a także późniejsze monitorowanie tejże wydajności. Monitoring pozwala na identyfikowanie zagrożeń dla stabilności działania aplikacji związanych ze stanem obciążenia systemu. W przypadku, gdy narzędzie wykorzystywane do monitoringu wydajności obejmuje przetwarzanie danych osobowych, należy zapewnić zgodność z obowiązującymi przepisami RODO;
 - 11) zapewnienie połączenia z Internetem o przepustowości co najmniej 500 Mbit bez limitu transferu oraz dobrego stanu technicznego zarówno dysków, jak i innych podzespołów koniecznych do prawidłowego funkcjonowania serwera/serwerów, które udostępnił Wykonawca na potrzeby portalu Zamawiającego;

- 12) zapewnienie bezpieczeństwa narzędzia SmartRadar;
 - 13) wdrożenia zabezpieczeń w postaci: firewall, IPS/IDS, WAF, ochronę przed atakami DDoS, system antywirusowy i antymalware,
 - 14) regularnego wykonywania kopii bezpieczeństwa, pozwalających na odtworzenie portalu oraz narzędzia co najmniej do 7 dni wstecz.
 - 15) zarządzanie dostępem do serwerów aplikacyjnych i baz danych obejmować będzie tworzenie kont użytkowników do elementów aplikacji takich jak: systemy operacyjne serwera aplikacyjnego, systemy operacyjne serwera bazy danych oraz utworzenie dla serwera aplikacyjnego i administratorów systemu dostępów do bazy danych. Każde konto będzie musiało zostać skonfigurowane poprzez nadanie odpowiednich uprawnień (poziomów dostępów). W ramach prac polegających na zarządzaniu dostępami będzie przygotowanie kont VPN pozwalających na zdalny dostęp do zasobów narzędzia SmartRadar;
 - 16) prowadzenie monitoringu logów aplikacyjnych oraz logów serwera w czasie pracy narzędzia SmartRadar, pozwalającego na identyfikowanie błędów działania narzędzia oraz stałe poprawianie zidentyfikowanych błędów. Do monitoringu logów oraz stanu aplikacji zostanie wykorzystane narzędzie Glowroot;
 - 17) informowanie Zamawiającego o ewentualnych włamaniach/naruszeniach bezpieczeństwa, zabezpieczeniu dowodów zdarzenia, powstrzymania naruszenia bezpieczeństwa oraz usunięcia skutków materializacji zagrożeń;
 - 18) sporządzanie na wniosek Zamawiającego okresowych raportów statystycznych z wykorzystaniem narzędzi do analizy statystyk portalu www (np. Smartlook, Mixpanel, Piwik, Leadfeeder lub o podobnych funkcjonalnościach, przy zachowaniu zgodności z przepisami RODO w przypadku wystąpienia przetwarzania danych osobowych);
 - 19) wykonywanie kopii zapasowych bazy danych. Kopie będą wykonywane w ustalonym cyklu, a pliki kopii bazy danych zarchiwizowane. Zakłada się, że częstotliwość wykonywania kopii zapasowych to cykl: kopia codzienna, tygodniowa i miesięczna;
 - 20) dostępność narzędzia SmartRadar na poziomie 99,0% w okresie jednego miesiąca.;
 - 21) w przypadku prowadzenia prac technicznych powodujących niedostępność narzędzia SmartRadar - informowanie Zamawiającego minimum na dwa dni robocze przed planowanymi pracami, wskazując czas na jaki istnieje prawdopodobieństwo niedostępności portalu oraz narzędzia;
 - 22) kompleksowe wsparcie/konsultacje techniczne i merytoryczne (udzielanie konsultacji dotyczących eksploatacji) narzędzia SmartRadar w czasie pracy Zamawiającego, tj. poniedziałek – piątek w godz. 8.15 – 16.15;
 - 23) rozwiązywanie problemów i usuwanie błędów zgłaszanych przez Zamawiającego w narzędziu SmartRadar, w formie telefonicznej, mailem lub za pośrednictwem dedykowanego internetowego systemu zgłoszeń, tj. w okresie poniedziałek – niedziela w godzinach 8.15 – 16.15; zakres zgłoszonych błędów będzie obejmował kwestie dotyczące poprawy działania narzędzia SmartRadar na poziomie funkcjonalnym jak i nie funkcjonalnym (np. zmiana konfiguracji);
 - 24) terminowe usuwanie zgłoszonych błędów:
 - a) 12 godzin od momentu jego zgłoszenia (błąd krytyczny) – za błąd krytyczny, uważa się każdy błąd uniemożliwiający dostęp do narzędzia SmartRadar, ich eksploatację, w tym brak możliwości wprowadzania i edycji treści oraz niepobierania danych ze wskazanych źródeł;
 - b) 3 dni robocze lub w innym zaakceptowanym przez obie strony terminie liczonym od momentu zgłoszenia przez Zamawiającego dla pozostałych błędów w czasie;
- W uzasadnionych przypadkach termin naprawy błędu może zostać przesunięty. Uzgodnienie innego terminu naprawy błędu będzie udokumentowane w formie notatki,

zawierającej informację o przyczynach zmiany terminu naprawy błędu, przygotowanej przez Wykonawcę i zaakceptowanej przez Zamawiającego;

- 25) na wniosek Zamawiającego - przeprowadzenie instruktażu dla administratorów Zamawiającego w wymiarze do 4 godzin;

Instruktaż zostanie przeprowadzony w siedzibie Zamawiającego lub zdalnie w zakresie konfiguracji usług. Dokładny zakres zostanie uzgodniony z Zamawiającym;

- 26) przygotowanie i przekazanie Zamawiającemu kopii narzędzia SmartRadar przed upływem zakończenia świadczenia usług stanowiących przedmiot zamówienia.

VI. WYMAGANIA TECHNICZNE DLA SMARTRADAR

1. Aplikacja SmartRadar używa 3 serwerów (VM). Jako system operacyjny wykorzystany jest Centos 7.x.

Nazwa	CPU	RAM	HDD
Serwer WEB	6	10	50 GB SSD
Serwer Aplikacyjny	6	10	50 GB SSD
Serwer Bazy Danych	6	12	50 GB SSD

2. Kod źródłowy aplikacji jest podzielony na dwie części, część aplikacji Java oraz część aplikacji Angular.
3. Do skompilowania aplikacji Java należy zapewnić zainstalowane oprogramowanie java8jdk oraz aplikację maven w wersji 3.3.9.
4. Aplikacja Angular (Frontend) - Frontend opracowany został za pomocą frameworka Angular 2 w wersji 8. Wymagane oprogramowanie to: nodejs -v 12.5.0 lub wyższe oraz npm.
5. Aplikacja Java (Backend) została opracowana za pomocą technologii Java oraz frameworka SpringBoot. Wymagane oprogramowanie to Maven w wersji 3.3.9.
6. Baza danych - wymagana baza danych to MariaDb w wersji 10.3.17.
7. Działanie serwera aplikacyjnego oraz bazy danych SmartRadar będzie oparte na systemie operacyjnym Centos w wersji 7 oraz silniku bazy danych MariaDb w wersji 5.5, serwer aplikacyjny wbudowany w narzędzie w wersji 9.
8. Oprogramowanie standardowe zainstalowane na serwerze aplikacyjnym i bazy danych będzie podlegało cyklicznej weryfikacji oraz aktualizacji.
9. Konfiguracja usług sieciowych ma na celu skonfigurowanie elementów infrastruktury sieciowej takich jak serwery proxy, loadbalancery, serwery WWW oraz inne wymagane składowe infrastruktury. Dodatkowo w ramach konfiguracji sieciowej zostanie zapewniona instalacja odpowiednich certyfikatów ssl. Konfiguracja usług sieciowych obejmie również konfigurację adresacji IP poszczególnych elementów infrastruktury.
10. Narzędzie SmartRadar umożliwi w tym samym czasie rzeczywistym dostęp dla 50 użytkowników przy założeniach, że dla każdego użytkownika maksymalny czas ładowania narzędzia z całą jej zawartością, w której zawierają się pliki kaskadowe arkuszy stylów, grafiki/obrazy, pliki skryptów wynosi do 15 sekund.
11. Mechanizm autoryzacji wymagający podania loginu i hasła.
12. Portal smart.gov.pl oraz narzędzie SmartRadar zostanie zabezpieczona przed najbardziej popularnymi podatnościami aplikacji internetowych takimi jak: „Sql Injection”, „xss”, „Broken Authentication”.
13. W celu zapewnienia bezpieczeństwa komunikacja pomiędzy przeglądarką internetową, a serwerem aplikacyjnym będzie odbywać się za pomocą szyfrowanego połączenia z wykorzystaniem zaufanych certyfikatów ssl.

14. Usługa obejmie obsługę awarii usług sieciowych, z których importowane są wartości wskaźników do zasobów narzędzia SmartRadar. Administrator będzie zobowiązany do zidentyfikowania powodu wystąpienia awarii. W przypadku błędu po stronie narzędzia SmartRadar, koniecznym będzie usunięcie usterki w ramach utrzymania.

VII. MIEJSCE I TERMIN SKŁADANIA OFERT

1. Ofertę należy przestać za pośrednictwem poczty elektronicznej **do dnia 5.06.2024r. do godz. 15:00**, na adres: wieslaw.smierzynski@mr.it.gov.pl oraz justyna.gorzoch@mr.it.gov.pl
2. Wykonawca jest zobowiązany do wskazania w ofercie terminu związania ofertą, nie krótszego niż 30 dni kalendarzowych.
3. Oferty dostarczone po terminie nie będą rozpatrywane.
4. W toku badania i oceny ofert Zamawiający może żądać od Oferentów wyjaśnień dotyczących treści zgłoszonych ofert.

VIII. WARUNKI UDZIAŁU W POSTĘPOWANIU

Za spełniających warunki udziału w postępowaniu Zamawiający uzna Wykonawców, którzy wykażą, że **w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonali dla podmiotów administracji publicznej usługi polegające na obsłudze co najmniej 3 portali internetowych związanych z otwartymi danymi publicznymi.**

IX. OCENA OFERT

Jedynym kryterium wyboru najkorzystniejszej oferty jest cena.

Klauzula informacyjna - RODO

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”, informujemy, że:

- Administratorem Pani/Pana danych osobowych jest Minister Rozwoju i Technologii, z siedzibą w Warszawie, Plac Trzech Krzyży 3/5, tel.: +48 222 500 123.
- Kontakt do Inspektora Ochrony Danych w Ministerstwie Rozwoju i Technologii: iod@mr.pit.gov.pl.
- Pani/Pana dane osobowe będą przetwarzane w celach: wyboru wykonawcy lub zawarcia i realizacji umowy.
- Dane osobowe mogą zostać ujawnione właściwym organom oraz podmiotom upoważnionym zgodnie z obowiązującym prawem.
- Dane osobowe są przetwarzane na podstawie:
 - art. 6 ust. 1 lit c RODO w celu wyboru wykonawcy,
 - art. 6 ust. 1 lit. b RODO w celu zawarcia oraz realizacji umowy
- Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów przetwarzania, w tym do czasu upływu okresu przedawnienia zobowiązania podatkowego wynoszącego 5 lat i nie krócej niż okres wskazany w przepisach o archiwizacji tj. ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2018 r. poz. 217 ze zm.).

- W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO.
- 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;
 - 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;
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (na adres: ul. Stawki 2, 00 - 193 Warszawa), gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
 - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c lub b RODO.