WIF-RIF.042.29.00002.2022 Gliwice, 2.12.2022 r.

ZAPYTANIE OFERTOWE

Przeprowadzenie diagnozy cyberbezpieczeństwa w Starostwie Powiatowym w Gliwicach związanej z realizacją projektu *Cyfrowy Powiat* w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Programu Operacyjnego Polska Cyfrowa na lata 2014-2020

Postępowanie prowadzone jest na podstawie art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2022 r. poz. 1710 z późn. zm.) o wartości szacunkowej poniżej 50 000 zł netto w oparciu o rozeznanie rynku zgodnie z zapisami *Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020*.

I. Nazwa i adres Zamawiającego:

Powiat Gliwicki
ul. Zygmunta Starego 17
44-100 Gliwice

Osoby do kontaktu:

W sprawach merytorycznych – Jacek Sulecki, tel. 32 332 66 21, j.sulecki@starostwo.gliwice.pl

W sprawach formalnych – Rafał Wojciechowski, tel. 32 338 37 18, r.wojciechowski@starostwo.gliwice.pl

II. Nazwa i adres miejsca realizacji przedmiotu zamówienia:

SPG – Starostwo Powiatowe w Gliwicach, ul. Zygmunta Starego 17, 44-100 Gliwice.

III. Wspólny słownik zamówień (CPV)

Kod CPV 72810000-1, Usługi audytu komputerowego
Kod CPV 79212000-3, Usługi audytu
Kod CPV 73431000-2, Testy i ocena sprzętu bezpieczeństwa
Kod CPV 72000000-5, Usługi informatyczne: konsultacyjne, opracowywanie oprogramowania, internetowe i wsparcia

IV. Przedmiot zamówienia

1. Przedmiotem zamówienia jest przeprowadzenie **diagnozy cyberbezpieczeństwa** zgodnie z zakresem oraz formularzem stanowiącym Załącznik nr 8 – *Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa* do Regulaminu Konkursu Grantowego *Cyfrowy Powiat* realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia. Ww. formularz został załączony jako **Załącznik nr 1** do zapytania ofertowego. Formularz należy wypełnić zgodnie z zaleceniami dotyczącymi sposobu wypełniania załącznika nr 8 oraz zaleceniami dotyczącymi sposobu wypełniania pól opisowych (tekstowych) w arkuszach KRI oraz CERT opisanymi w dokumencie pn. *Diagnoza Cyberbezpieczeństwa – zalecenia dotyczące zasad wypełniania i wysyłania do NASK dokumentów w ramach konkursu grantowego „Cyfrowy Powiat"* opracowanym przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
   UWAGA! W przypadku zmiany formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa przez administratora Projektu, Wykonawca zobligowany będzie wykonać zamówienie z uwzględnieniem jego aktualnej wersji.
   Link do pobrania załącznika: https://www.gov.pl/attachment/64b72499-f968-44a6-b4c0-8b99345616de
2. Diagnoza musi być przeprowadzona przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Wykaz certyfikatów uprawniających do przeprowadzania audytu (jeden z poniższych):
   a) Certified Internal Auditor (CIA);
   b) Certified Information System Auditor (CISA);
   c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
   d) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
   e) Certified Information Security Manager (CISM);
   f) Certified in Risk and Information Systems Control (CRISC);
   g) Certified in the Governance of Enterprise IT (CGEIT);
   h) Certified Information Systems Security Professional (CISSP);
   i) Systems Security Certified Practitioner (SSCP);
   j) Certified Reliability Professional;
   k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
3. Składana oferta powinna obejmować cały zakres przedmiotu zamówienia tj. obejmować wykonanie wszystkich prac i czynności związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa według Załącznika nr 8 – *Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa* do Regulaminu Konkursu Grantowego *Cyfrowy Powiat*.
4. Szczegółowy zakres przedmiotu zamówienia został określony w **Załączniku nr 1** do zapytania.
5. Wykonawca zobowiązany jest do kompleksowej realizacji zamówienia tzn. wykonania diagnozy cyberbezpieczeństwa, wypełnienia i podpisania wymaganych dokumentów zgodnie z Regulaminem

Konkursu Grantowego Cyfrowy Powiat i zapisami umowy o powierzenie grantu oraz ich dostarczenia w wersji elektronicznej i papierowej do siedziby Zamawiającego (po jednym egzemplarzu).

6. Przeprowadzenie diagnozy cyberbezpieczeństwa nastąpi w siedzibie Zamawiającego. Zamawiający nie dopuszcza możliwości realizacji usługi za pomocą środków komunikacji zdalnej.
7. Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym kosztów ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanowania dokumentów.
8. Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji na każdym etapie realizacji zamówienia, aż do zaakceptowania dokumentów wystawionych przez Grantodawcę Konkursu Cyfrowy Powiat.

V. Termin wykonania zamówienia oraz warunki płatności

1. Termin realizacji usługi wynosi 30 dni od dnia podpisania umowy, z zastrzeżeniem, iż maksymalny wymagany termin dla wykonania przedmiotu zamówienia to 31 stycznia 2023 r.
2. Usługa będzie realizowana w dni robocze w godzinach pracy urzędu tj. poniedziałek-środa godz. 7.30-15.30, czwartek godz. 7.30-17.30, piątek godz. 7.30-13.30.
3. W przypadku stwierdzenia, że przedmiot dostawy ma wady lub jest niezgodny z zamówieniem, Zamawiający ma prawo odmówić odbioru do czasu zaoferowania przedmiotu dostawy zgodnego z zamówieniem lub wolnego od wad.
4. Podstawą do wystawienia faktury będzie protokół odbioru przedmiotu zamówienia (na wzorze Zamawiającego) bez zastrzeżeń, podpisany przez Wykonawcę oraz przedstawiciela Zamawiającego.
5. Wymagany termin płatności wynosi **30 dni** od daty wpływu prawidłowo wystawionej faktury do Zamawiającego. **Faktura wystawiona będzie nie wcześniej niż w dniu 1 stycznia 2023 r. na: Powiat Gliwicki, ul. Zygmunta Starego 17, 44-100 Gliwice, NIP: 631 26 06 158.**
6. Płatność będzie dokonywana wyłącznie na firmowy rachunek bankowy kontrahenta służący do prowadzenia działalności gospodarczej.

VI. Informacje uzupełniające

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie dopuszcza składania ofert wariantowych.
3. Zamawiający nie dopuszcza możliwości udzielenia zamówień dodatkowych.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu oraz zwrotu ofert złożonych w terminie.
5. Zamawiający nie przewiduje udzielania zaliczek na poczet wykonania zamówienia.
6. Zamawiający nie dopuszcza prowadzenia rozliczeń w walutach obcych.
7. Postępowanie w całości prowadzone jest w języku polskim, włącznie z wszelką korespondencją oraz innymi formami porozumiewania się Zamawiającego z Wykonawcą.

VII. Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1. posiadają wiedzę i doświadczenie w realizacji usług będących przedmiotem zapytania lub podobnych, na wstępne potwierdzenie powyższego Wykonawca dołączy **wykaz zrealizowanych usług** (według wzoru składającego się na Formularz ofertowy), potwierdzających wykonanie w ciągu 3 lat poprzedzających złożenie oferty, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – co najmniej 2 diagnoz/audytów cyberbezpieczeństwa realizowanych w ramach Konkursu Grantowego „Cyfrowa Gmina" lub co najmniej 3 audytów bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie. Przez „podobny zakres" Zamawiający rozumie wykonanie audytu lokalnych sieci teleinformatycznych, serwisów pocztowych i WWW, organizacji zarządzania bezpieczeństwem teleinformatycznym.
   Zamawiający wezwie Wykonawcę najwyżej ocenionego i nie podlegającego odrzuceniu do złożenia dowodów określających czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa są referencje odbiorców tych usług lub inne dokumenty potwierdzające należyte wykonanie tych usług. W przypadku niezłożenia przez Wykonawcę dokumentów w wyznaczonym terminie, nie krótszym niż 2 dni, oferta Wykonawcy podlegać będzie odrzuceniu;
2. do realizacji zamówienia wskażą co najmniej 1 osobę legitymującą się odpowiednimi certyfikatami do realizacji przedmiotu zamówienia – na wstępne potwierdzenie Wykonawca dołączy **listę osób skierowanych do realizacji usługi** (według wzoru składającego się na Formularz ofertowy) potwierdzającą posiadanie wymaganych kwalifikacji, o których mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
   Zamawiający wezwie Wykonawcę najwyżej ocenionego i nie podlegającego odrzuceniu do złożenia dowodów określających czy te osoby legitymują się odpowiednimi uprawnieniami, przy czym dowodami, o których mowa będą kopie certyfikatów, o których mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W przypadku niezłożenia przez Wykonawcę dokumentów w wyznaczonym terminie, nie krótszym niż 2 dni, oferta Wykonawcy podlegać będzie odrzuceniu;

VIII. Opis sposobu przygotowania oferty

1. Składana oferta powinna obejmować cały zakres przedmiotu zamówienia tj. obejmować wykonanie wszystkich prac i czynności związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa. Treść oferty musi odpowiadać treści niniejszego zapytania, pod rygorem odrzucenia oferty.
2. Wykonawca składa ofertę na Formularzu ofertowym stanowiącym **Załącznik nr 2** do zapytania. W przypadku nieskorzystania z Formularza, oferta musi zawierać wszystkie wymagane w jego wzorze informacje, oświadczenia. Do oferty załącza się dokument pełnomocnictwa, jeżeli reprezentacja Wykonawcy nie wynika z publicznie dostępnych wykazów (KRS, CEIDG).
3. Cena w ofercie musi być określona w PLN jako cena netto oraz brutto (liczbowo) wraz ze wskazaniem wartości podatku VAT. W zaoferowanej cenie brutto realizacji zamówienia muszą być

zawarte wszelkie opłaty, podatki, cła i inne zobowiązania wynikające ze stosownych ustaw, koszty ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanowania dokumentów.

4. Koszty związane z przygotowaniem oferty ponosi składający ofertę.

IX. Miejsce i termin złożenia oferty

1. Ofertę należy złożyć w nieprzekraczalnym terminie do dnia **9 grudnia 2022 r. do godz. 10.00** w formie skanu wypełnionego i podpisanego formularza ofertowego na skrzynkę e-mailową r.wojciechowski@starostwo.gliwice.pl **Decyduje data wpływu do Zamawiającego (na skrzynkę e-mail).**
2. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać ofertę.
3. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty należy złożyć według takich samych zasad jak złożenie oferty z dopiskiem w tytule wiadomości „ZMIANA" lub „WYCOFANIE".
4. W przypadku złożenia oferty po terminie Zamawiający niezwłocznie zawiadomi Wykonawcę o złożeniu oferty po terminie.
5. Zamawiający dokona oceny złożonych ofert i ustali ich kolejność według kryterium cenowego wskazanego w sekcji XII.
6. Zamawiający uprawniony jest do żądania przedstawienia wyjaśnień w stosunku do treści złożonej oferty lub składanych dokumentów.

X. Wyjaśnienia treści zapytania ofertowego

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert.
2. Jeżeli wniosek o wyjaśnienie treści zapytania ofertowego wpłynie do Zamawiającego później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert lub dotyczy udzielonych już wyjaśnień, Zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.
3. Zamawiający, w uzasadnionych przypadkach, zastrzega sobie prawo do zmiany treści zapytania ofertowego przed upływem terminu składania ofert. Wprowadzone w ten sposób zmiany treści, uzupełnienia i ustalenia lub zmiany, w tym zmiany terminów zostaną niezwłocznie opublikowane w Biuletynie Informacji Publicznej w zakładce dot. zapytania.

XI. Termin związania ofertą

1. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca pozostaje związany ofertą przez okres 30 dni od upływu terminu składania ofert.

XII. Kryteria stosowane przy ocenie oferty

1. Szczegółowo rozpatrywane przez Zamawiającego będą oferty, które:
   a) spełniają wymagania określone w niniejszym zapytaniu ofertowym i są zgodne co do treści z wymaganiami Zamawiającego,
   b) zostały złożone w terminie.
2. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Kryterium	Waga [%]	Maksymalna liczba punktów	Sposób oceny według wzoru
Cena brutto za wykonanie przedmiotu zamówienia	100%	100	Cena najtańszej oferty C= ---------- x 100 pkt Cena badanej oferty
RAZEM	**100%**	**100 pkt**	

3. Wszystkie kwoty w ofercie należy podać w zaokrągleniu do pełnych groszy (dwóch miejsc po przecinku).
4. Ocena punktowa w kryterium „Cena brutto za wykonanie przedmiotu zamówienia" dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej (wynikająca z działania punktacja zostanie zaokrąglona do dwóch miejsc po przecinku).
   Maksymalna liczba punktów w tym kryterium – **100 pkt.**
5. Jako najkorzystniejsza zostanie uznana oferta Wykonawcy, która otrzyma największą całkowitą liczbę punktów, wyliczoną zgodnie z wzorem wskazanym w ust. 2.
6. Zamawiający udzieli zamówienia Wykonawcy, którego oferta jest zgodna z treścią zapytania oraz została oceniona jako najkorzystniejsza w oparciu o podane powyżej kryteria wyboru.
7. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na fakt, że dwie lub więcej ofert przedstawia taki sam bilans ceny i pozostałych kryteriów oceny ofert, Zamawiający wezwie Wykonawców do złożenia ofert dodatkowych, z zastrzeżeniem, iż oferty te nie mogą przedstawiać gorszych warunków od proponowanych pierwotnie.
8. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania bez podania uzasadnienia, a także do pozostawienia postępowania bez wyboru oferty, w szczególności w sytuacji, gdy cena najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia oraz prawo do odpowiedzi tylko na wybraną ofertę, do negocjacji warunków przy wyborze oferty, a także rezygnacji z udzielenia zamówienia bez podania przyczyny.

XIII. Informacje dotyczące zawarcia umowy po wyborze oferty i istotnych postanowieniach

1. Wzór umowy stanowi **Załącznik nr 3** do zapytania.
2. W przypadku uchylania się od podpisania umowy przez Wykonawcę, którego oferta została wybrana w toku postępowania, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzania ich ponownej oceny.

XIV. Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XV. Klauzule informacyjne

Zgodnie z art. 13 ust. 1 i ust. 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 osobowych) informujemy, iż:

1) administratorem Pana danych osobowych jest Starosta Gliwicki z siedzibą w Gliwicach przy ul. Zygmunta Starego 17;
2) kontakt z Inspektorem Ochrony Danych – tel. 32 231 96 86, e-mail: iod@starostwo.gliwice.pl;
3) Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. w celu zawarcia umowy / realizacji zamówienia;
4) odbiorcami Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz firma LTC Sp. z o.o. z Wielunia, Kancelaria Prawna COMESTOR Radca Prawny Ireneusz Żarłok z siedzibą w Mysłowicach oraz Kancelaria Młynarczyk, Laburda, Augustyniak Kancelaria Radców Prawnych Sp. p. z siedzibą w Zabrzu;
5) Pana dane osobowe będą przechowywane przez okres wynikający z przepisów prawa tj. Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych;
6) posiada Pan prawo żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania oraz prawo do ograniczenia ich przetwarzania;
7) przysługuje Panu prawo wniesienia skargi do organu nadzorczego, tj. do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pan, iż przetwarzanie Pana danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych wskazanego na wstępie;
8) podanie danych osobowych w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego i podpisanie umowy z wybranym podmiotem jest obligatoryjne;
9) Pana dane nie będą przekazywane odbiorcy w państwie trzecim lub organizacji międzynarodowej;
10) Pana dane nie będą poddawane zautomatyzowanemu podejmowaniu decyzji (profilowaniu).

Niniejsze postępowanie stanowi element realizacji projektu *Cyfrowy Powiat* w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Programu Operacyjnego Polska Cyfrowa na lata 2014-2020. Na podstawie Umowy o powierzenie grantu o numerze 5466/P/2022 Zamawiającemu (Powiatowi Gliwickiemu) powierzono przetwarzanie Danych osobowych w imieniu i na rzecz administratora. Wykonując obowiązek informacyjny wynikający z art. 13 i 14 RODO Zamawiający przedstawia poniższą klauzulę informacyjną administratora.

Ze względu na to, że **to Minister Funduszy i Polityki Regionalnej - jako Instytucja Zarządzająca POPC 2014-2020** - określa: jakie dane osobowe, w jaki sposób i w jakim celu będą przetwarzane w związku z realizacją Programu, **pełni on rolę administratora danych osobowych przetwarzanych w związku z realizacją POPC 2014-2020** w rozumieniu RODO [Rozporządzenie 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1).].

Przy czym jest on administratorem zarówno wobec danych osobowych, które samodzielnie pozyskał, jak i wobec danych osobowych pozyskanych przez inne podmioty zaangażowane w realizację Programu (tj. przez innych administratorów, którzy w tym przypadku pełnią dodatkowo funkcję podmiotów przetwarzających dane osobowe [Podmiotami przetwarzającymi są: Instytucja Pośrednicząca POPC 2014-2020, beneficjenci oraz inne podmioty zaangażowane w realizację POPC 2014-2020, którym Minister (lub inny upoważniony podmiot) powierzył przetwarzanie danych osobowych w ramach POPC 2014-2020]).

Minister Funduszy i Polityki Regionalnej jest także administratorem danych osobowych, które przetwarza jako beneficjent projektów współfinansowanych ze środków POPC 2014-2020.

Minister Funduszy i Polityki Regionalnej jest również administratorem danych zgromadzonych w zarządzanym przez niego **Centralnym Systemie Teleinformatycznym** wspierającym realizację POPC 2014-2020.

I. Cel przetwarzania danych osobowych

Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe **w celu realizacji zadań przypisanych Instytucji Zarządzającej POPC 2014-2020**, w zakresie w jakim jest to niezbędne dla realizacji tego celu. Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe **w szczególności w celach**:

1. udzielania wsparcia beneficjentom ubiegającym się o dofinansowanie i realizującym projekty,
2. potwierdzania kwalifikowalności wydatków,
3. wnioskowania o płatności do Komisji Europejskiej,
4. raportowania o nieprawidłowościach,
5. ewaluacji,
6. monitoringu,
7. kontroli,
8. audytu,
9. sprawozdawczości oraz
10. działań informacyjno-promocyjnych.

II. Podstawy prawne przetwarzania

Przetwarzanie danych osobowych w związku z realizacją POPC 2014-2020 odbywa się zgodnie z RODO.

Podstawą prawną przetwarzania danych jest konieczność **realizacji obowiązków spoczywających na Ministrze Funduszy i Polityki Regionalnej - jako na Instytucji Zarządzającej - na podstawie przepisów prawa europejskiego i krajowego** (art. 6 ust. 1 lit. c RODO).

Obowiązki te wynikają m.in. z przepisów ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 oraz przepisów prawa europejskiego:

1. rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego,

oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006,

2. rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi.

Podstawą przetwarzania danych osobowych przez Ministra są również:

1. **konieczność realizacji umowy**, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b RODO) - podstawa ta ma zastosowanie m. in. do danych osobowych osób prowadzących samodzielną działalność gospodarczą, z którymi Minister zawarł umowy w celu realizacji POPC 2014-2020,
2. wykonywanie **zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej Ministrowi (art. 6 ust. 1 lit e RODO) - podstawa ta ma zastosowanie m. in. do organizowanych przez Ministra konkursów i akcji promocyjnych dotyczących Programu,
3. uzasadniony interes prawny Ministra Funduszy i Polityki Regionalnej (art. 6 ust. 1 lit f RODO) – podstawa ta ma zastosowanie m.in. do danych osobowych przetwarzanych w związku z realizacją umów w ramach Funduszy Europejskich.

W ramach POPC 2014-2020 **w działaniu 3.1** - Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych przetwarzane są **dane szczególnej kategorii** (dane o niepełnosprawności). Podstawą prawną ich przetwarzania **jest wyraźna zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit a RODO)**.

III. Rodzaje przetwarzanych danych

Minister Funduszy i Polityki Regionalnej w celu realizacji POPC 2014-2020 przetwarza dane osobowe m. in.:

1. pracowników, wolontariuszy, praktykantów i stażystów reprezentujących lub wykonujących zadania na rzecz podmiotów zaangażowanych w obsługę i realizację POPC 2014-2020,
2. osób wskazanych do kontaktu, osób upoważnionych do podejmowania wiążących decyzji oraz innych osób wykonujących zadania na rzecz wnioskodawców, beneficjentów i partnerów,
3. uczestników szkoleń, konkursów, konferencji, komitetów monitorujących, grup roboczych, grup sterujących oraz spotkań informacyjnych lub promocyjnych organizowanych w ramach POPC 2014-2020,
4. kandydatów na ekspertów oraz ekspertów zaangażowanych w proces wyboru projektów do dofinansowania lub wykonujących zadania związane z realizacją praw i obowiązków właściwych instytucji, wynikających z zawartych umów o dofinansowanie projektów,
5. osób, których dane będą przetwarzane w związku z badaniem kwalifikowalności środków w projekcie, w tym w szczególności: personelu projektu, uczestników komisji przetargowych, oferentów i wykonawców zamówień publicznych, osób świadczących usługi na podstawie umów cywilnoprawnych.

Wśród **rodzajów danych osobowych** przetwarzanych przez Ministra można wymienić:

1. dane identyfikacyjne, w szczególności: imię, nazwisko, miejsce zatrudnienia/formę prowadzenia działalności gospodarczej, stanowisko; w niektórych przypadkach także nr PESEL/NIP/REGON,
2. dane dotyczące stosunku pracy, w szczególności otrzymywane wynagrodzenie oraz wymiar czasu pracy,
3. dane kontaktowe, które obejmują w szczególności adres e-mail, nr telefonu, nr fax, adres do korespondencji,
4. dane o charakterze finansowym, w szczególności nr rachunku bankowego, kwotę przyznanych środków, informacje dotyczące nieruchomości (nr działki, nr księgi wieczystej, nr przyłącza gazowego), kwotę wynagrodzenia,
5. dane zbierane w celu realizacji obowiązków sprawozdawczych do których realizacji zobowiązane są państwa członkowskie, obejmujące w szczególności: płeć, wiek w chwili przystąpienia do projektu, wykształcenie, wykonywany zawód, narodowość, informacje o niepełnosprawności.

Dane pozyskiwane są bezpośrednio od osób, których dane dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację programów operacyjnych, w szczególności wnioskodawców, beneficjentów i partnerów.

W przypadku, gdy dane pozyskiwanie są bezpośrednio od osób, których dane dotyczą, podanie danych jest dobrowolne. Odmowa podania danych jest jednak równoznaczna z brakiem możliwości podjęcia stosownych działań, np. ubiegania się o środki w ramach POPC 2014-2020.

IV. Okres przechowywania danych

Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie **przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach POPC 2014-2020** - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

W niektórych przypadkach, np. prowadzenia kontroli u Ministra przez organy Unii Europejskiej, okres ten może zostać wydłużony.

V. Odbiorcy danych

Odbiorcami danych osobowych mogą być:

- podmioty, którym Instytucja Zarządzająca POPC 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności **Instytucja Pośrednicząca POPC**, a także **eksperci, podmioty prowadzące audyty, kontrole, szkolenia i ewaluacje**,
- **instytucje, organy i agencje Unii Europejskiej (UE)**, a także inne podmioty, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem POPC 2014-2020,
- podmioty świadczące na rzecz Ministra usługi związane z obsługą i rozwojem systemów teleinformatycznych oraz zapewnieniem łączności, w szczególności **dostawcy rozwiązań IT i operatorzy telekomunikacyjni**.

VI. Prawa osoby, której dane dotyczą

Osobom, których dane przetwarzane są w związku z realizacją POPC 2014-2020 przysługują następujące prawa:

1. prawo **dostępu do danych osobowych i ich sprostowania.** Realizując te prawo, osoba której dane dotyczą może zwrócić się do Ministra z pytanie m.in. o to czy Minister przetwarza jej dane osobowe, jakie dane osobowe przetwarza i skąd je pozyskał, jaki jest cel przetwarzania i jego podstawa prawna oraz jak długo dane te będą przetwarzane.
   W przypadku, gdy przetwarzane dane okażą się nieaktualne, osoba, której dane dotyczą może zwrócić się do Ministra z wnioskiem o ich aktualizację;
2. prawo **usunięcia lub ograniczenia ich przetwarzania** – jeżeli spełnione są przesłanki określone w art. 17 i 18 RODO. Żądanie usunięcia danych osobowych realizowane jest w szczególności gdy dalsze przetwarzanie danych nie jest już niezbędne do realizacji celu Ministra lub dane osobowe były przetwarzane niezgodnie z prawem. Szczegółowe warunki korzystania z tego prawa określa art. 17 RODO. Ograniczenie przetwarzania danych osobowych powoduje, że Minister może jedynie przechowywać dane osobowe. Minister nie może przekazywać tych danych innym podmiotom, modyfikować ich ani usuwać. Ograniczanie przetwarzania danych osobowych ma charakter czasowy i trwa do momentu dokonania przez Ministra oceny, czy dane osobowe są prawidłowe, przetwarzane zgodnie z prawem oraz niezbędne do realizacji celu przetwarzania. Ograniczenie przetwarzania danych osobowych następuje także w przypadku wniesienia sprzeciwu wobec przetwarzania danych – do czasu rozpatrzenia przez Ministra tego sprzeciwu;
3. prawo **wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;**
4. prawo do **cofnięcia zgody**, w każdym momencie - w przypadku, gdy podstawą przetwarzania danych jest zgoda (art. 9 ust. 2 lit a RODO). Cofnięcie zgody nie spowoduje, że dotychczasowe przetwarzanie danych zostanie uznane za niezgodne z prawem;
5. prawo **otrzymania danych osobowych w ustrukturyzowanym powszechnie używanym formacie**, przenoszenia tych danych do innych administratorów lub żądania, o ile jest to technicznie możliwe, przesłania ich przez administratora innemu administratorowi - w przypadku, gdy podstawą przetwarzania danych jest zgoda lub realizacja umowy z osobą, której dane dotyczą (art. 6 ust. 1 lit b RODO);
6. **prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych** - w przypadku, gdy podstawą przetwarzania danych jest realizacja zadań publicznych administratora lub jego prawnie uzasadnionych interesów (art. 6 ust. 1 lit e lub f RODO). Wniesienie sprzeciwu powoduje zaprzestanie przetwarzania danych osobowych przez Ministra, chyba że wykaże on, istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

VII. Zautomatyzowane podejmowanie decyzji

Dane nie podlegają procesowi zautomatyzowanego podejmowania decyzji.

VIII. Kontakt z Inspektorem Ochrony Danych

Ministerstwo Funduszy i Polityki Regionalnej ma swoją siedzibę pod adresem: ul. Wspólna 2/4, 00-926 Warszawa.

W przypadku pytań, kontakt z Inspektorem Ochrony Danych MFiPR jest możliwy:

- pod adresem: ul. Wspólna 2/4, 00-926 Warszawa,

pod adresem poczty elektronicznej: IOD@mfipr.gov.pl

Niniejszym oświadczam, iż zapoznałem się z powyższymi klauzulami informacyjnymi.

Składając ofertę, oferent jest zobowiązany wypełnić obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyska i przekaże w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

Załączniki do zapytania ofertowego:

1. Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa
2. Formularz ofertowy
3. Wzór umowy