nr sprawy **ROI.21.04.2022** **Załącznik nr 3 do Regulaminu**

ZAPYTANIE OFERTOWE

pieczęć Wydziału / Referatu

Zakup oprogramowania oraz przeprowadzenie szkoleń oraz audytu cyberbezpieczeństwa w ramach programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020 Działanie Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

1. TRYB ZAMÓWIENIA

Postępowanie prowadzone jest zgodnie z procedurami określonymi w Wytycznych w zakresie Kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 zgodnie z zasadą konkurencyjności.

Wspólny Słownik Zamówień:

48000000-8: pakiety oprogramowania i systemy informatyczne

72800000-8: usługi audytu komputerowego i testowanie komputerów

80420000-4: usługi e-lerning

2. OPIS PRZEDMIOTU ZAMÓWIENIA

W ramach *Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020 Działanie Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00* Urząd Miejski w Świdnicy zleca diagnozę cyberbezpieczeństwa i przeprowadzanie szkoleń dla pracowników Urzędu Miejskiego w Świdnicy jako **Zadanie nr 1** i/lub dostarczenie licencji narzędzi do analizy bezpieczeństwa styku sieci i Internetu, licencji zabezpieczających zdalny dostęp oraz szkolenie z administracji urządzeniami sieciowymi dla kadry informatycznej jako **Zadanie nr 2** i/lub dostarczenie oprogramowania do inwentaryzacji jako **Zadanie nr 3**, zgodnie z poniższą specyfikacją.

Zadanie nr 1:

Lp.	Nazwa	Ilość	Uwagi
1.	**Diagnoza cyberbezpieczeństwa:** Diagnoza musi zostać przeprowadzona przez osobę	1 szt.	**Termin dostarczenia**

	posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. Diagnoza ma obejmować niezbędne obszary w związku z przyznaniem Grantu w projekcie „Cyfrowa Gmina" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego, Program Operacyjny Polska Cyfrowa (POPC) na lata 2014-2020, pakiet REACT-UE Usługa ma być przeprowadzona w siedzibie Zmawiającego lub zdalnie. Efektem realizacji diagnozy będzie raport w formie **Załącznika nr 8 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa** – *Regulaminu Konkursu Grantowego Cyfrowa Gmina 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 Program Operacyjny Polska Cyfrowa na lata 2014 – 2020* z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie elektronicznej i papierowej. **Zakres diagnozy zawarty jest w załączniku nr 8 *Regulaminu Konkursu Grantowego Cyfrowa Gmina.***		**raportu: maksymalnie do dnia 22.07.2022 r.**
2.	**Szkolenie z cyberbezpieczeństwa:** - szkolenie zdalne, - około 270 pracowników, - 3 lub 4 tury, - zakres szkolenia: minimum: szkolenie skierowane do JST, cyberbezpieczeństwo w miejscu pracy i w pracy zdalnej, rozpoznawanie i zapobieganie oszustwom internetowym, bezpieczne korzystać z mediów społecznościowych, ochrona konta służbowego, metody zwiększające bezpieczeństwo, studium przypadków, inne.	1 szt.	

Zadanie nr 2:

Lp.	Nazwa	Ilość	Uwagi
1.	**Token FortiGate dla urządzeń mobilnych:** Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses (Urząd posiada urządzenia Fortigate stąd potrzeba oprogramowania producenta urządzenia).	30 licencji	Licencja elektroniczna
2.	**Analizator:** Środowisko pracy: VMware 6.5. FortiAnalizer-VM (2 GB/Day of Logs and 1 TB storage capacity) wraz z 24x7 FortiCare Contract (for 1-6 GB/Day of	1 szt.	wspiera VMware ESXi versions 5.0, 5.5, 6.0, 6.5 , 6.7, and 7.0,Microsoft Hyper-V

	Logs) (wsparcie obejmujące 30.09.2023 r. (Urząd wykorzystuje środowisko VMware oraz urządzenia Fortigate i stąd potrzeba analizatora producenta urządzenia w danym środowisku pracy)		Server 2012, 2016, and 2019
3.	**Szkolenie z administracji urządzeniami sieciowymi:** Voucher (ważny minimum do grudnia 2022 r.): Szkolenie NSE4 - FortiGate I Security - 3 dni - szkolenie zdalne w języku polskim (Urząd posiada urządzenia Fortigate stąd potrzeba szkolenia z oprogramowania producenta urządzenia)	1 szt.	

Zadanie nr 3

Lp.	Nazwa	Ilość	Uwagi
1.	**Aktualizacja oprogramowania:** Aktualizacja do najnowszej wersji oprogramowania Axence nVision, moduł Network dla nielimitowanej liczby urządzeń oraz moduły Inventory, Users, DataGuard umożliwiające zarządzanie 200 stacjami roboczymi (aktualizacja z wersji 8 Pro). (Urząd posiada oprogramowanie Axence stąd potrzeba licencji tego producenta).	200 licencji	Środowisko pracy dla serwera oprogramowania: Windows Serwer 2012 R2, 2016, 2019
2.	**Rozszerzenie licencji:** Zakup licencji najnowszego oprogramowania Axence nVision: moduły Inventory, Users, DataGuard umożliwiające zarządzanie stacjami roboczymi (z 200 posiadanych licencji do 320 - (Urząd posiada oprogramowanie Axence stąd potrzeba licencji tego producenta).	120 licencji	Środowisko pracy dla serwera oprogramowania: Windows Serwer 2012 R2, 2016, 2019

3. TERMIN REALIZACJI ZAMÓWIENIA:

3.1. Dla zadania 1

3.1.1.pkt. 1 : Termin dostarczenia raportu: maksymalnie do dnia 22.07.2022 r.

3.1.2.pkt. 2 : do 15.11.2022

3.2. Dla zadania 2 : do 30 dni od dnia podpisania umowy

3.3. Dla zadania 3 : do 30 dni od dnia podpisania umowy

4. KRYTERIA OCENY OFERT:
Cena – 100%

5. WARUNKI PŁATNOŚCI:
Przelew do 28 dni od daty wystawienia faktury.

6. OKRES UDZIELONEJ GWARANCJI:[1]
Zgodny ze standardami producentów.

[1] o ile jest wymagana

7. WARUNKI STAWIANE WYKONAWCY:

a) posiadanie uprawnienia do wykonywania określonej działalności lub czynności.
b) posiadanie wiedzy i doświadczenia do wykonania zamówienia.
c) dysponowanie odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia.
d) sytuacja ekonomiczna i finansowa zapewniająca wykonanie zamówienia.
e) dostarczone licencje i oprogramowanie muszą być fabrycznie nowe oraz nieużywane. Zamawiający w momencie odbioru licencji i oprogramowania przewiduje możliwość zastosowania procedury sprawdzającej legalność dostarczonego oprogramowania. Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości co do jego legalności.

8. WYKAZ DOKUMENTÓW POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW, KTÓRE MAJĄ BYĆ ZAŁĄCZONE DO OFERTY:

a) oświadczenie wykonawcy o spełnieniu warunków udziału dokumentów postępowaniu wg wzoru – załącznik nr 4 do zapytania ofertowego,
b) kopia uprawnień wykazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu osoby przeprowadzającej diagnozę cyberbezpieczeństwa – dotyczy Zadania nr 1 punkt 1,
c) aktualny odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej,
d) parafowany projekt umowy – załącznik nr 1a, 1b, 1c (w zależności od zadania).

9. SPOSÓB SKŁADNIA OFERT:

a) Ofertę sporządzoną w języku polskim należy złożyć poprzez platformę Baza Konkurencyjności - https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

lub:

b) Ofertę w formie pisemnej w języku polskim należy złożyć w zamkniętej kopercie zaadresowanej „Zapytanie ofertowe ROI.21.04.2022 - *Zakup oprogramowania oraz przeprowadzenie szkoleń oraz audytu cyberbezpieczeństwa*".[2]

10. TERMIN SKŁADANIA OFERT: do 27.05.2022 r. do godziny $11^{\underline{00}}$

11. MIEJSCE SKŁADANIA OFERT:

11.1. Platforma Baza Konkurencyjności - https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

lub

11.2. Urząd Miejski w Świdnicy, ul. Armii Krajowej 49, 58-100 Świdnica[3]

12. DANE ZAMAWIAJĄCEGO:
Urząd Miejski w Świdnicy
ul. Armii Krajowej 49
58-100 Świdnica
e-mail: informatyk@um.swidnica.pl
tel.: 74 8562 922, 74 8562 908, 74 8562 932, 74 8562 931

[2] w przypadku składania oferty w formie pisemnej
[3] w przypadku składania oferty w formie pisemnej

13. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W PROGRAMIE POLSKA CYFROWA 2014-2020 (POPC 2014-2020)

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

14. ZAŁĄCZNIKI:

- projekty umów - załącznik nr 1a, 1b, 1c[4].
- wzór oferty – załącznik nr 3
- oświadczenie o spełnieniu warunków udziału w postępowaniu wg wzoru – załącznik nr 4
- załącznik nr 8 Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa do regulaminu Konkursu Grantowego Cyfrowa Gmina 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 Program Operacyjny Polska Cyfrowa na lata 2014 – 2020

Świdnica, dnia 18 maja 2022 r.

Sekretarz Miasta Świdnicy
Maciej Rataj

MACIEJ RATAJ; GMINA MIASTO ŚWIDNICA

Elektronicznie podpisany przez MACIEJ RATAJ; GMINA MIASTO ŚWIDNICA
Data: 2022.05.19 15:21:04 +02'00'

[4] o ile jest wymagany