

ZAPYTANIE OFERTOWE – DI/9/3/22

„Wykonanie audytu bezpieczeństwa teleinformatycznego, doradztwo w zakresie cyberbezpieczeństwa oraz ochrony informacji dla operatora usługi kluczowej”

I. PODSTAWA PRAWNA

Zamówienia klasyczne poniżej progu określonego w art. 2 ust.1 pkt ustawy Prawo zamówień publicznych (Dz.U 2019 poz. 2019) oraz na podstawie art. 44 ust. 2 ustawy o finansach publicznych (Dz.U. 2019 poz. 869), zwracamy się z zapytaniem ofertowym.

II. PRZEDMIOT ZAMÓWIENIA ORAZ ISTOTNE WARUNKI ZAMÓWIENIA

1. Opis przedmiotu zamówienia:

1. Doradztwo w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej

- przygotowanie we współpracy ze Szpitalem dokumentacji dotyczącej:
 - a) systemu zarządzania bezpieczeństwem informacji Zleceniodawcy, wytworzonej zgodnie z wymaganiami normy PN-EN ISO/IEC 27001,
 - b) systemu zarządzania ciągłością działania usługi Zleceniodawcy, wytworzonej zgodnie z wymaganiami normy PN-EN ISO 22301;
- doradztwo osobie wyznaczonej przez operatora usługi kluczowej i będącej odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w sprawach wymagających wykonywania obowiązków wobec tych podmiotów;
- doradztwo wobec powołanej przez operatora usługi kluczowej wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo w podejmowanych czynnościach i wykonywanych zadaniach nałożonych obowiązkami prawnymi Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2020 r., poz. 1369) – zwanej dalej „Ustawą KSC” – tj. w zakresie dotyczącym:
 - a) zarządzania incydentami oraz obsłudze incydentów;
 - b) eliminacji podatności systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
 - c) współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo z właściwym CSIRT w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
- świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT – w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
- świadczenie pomocy w przygotowaniu zgłoszenia informacji o innych incydentach, zagrożeniach cyberbezpieczeństwa, szacowaniu ryzyka, podatnościach lub wykorzystywanych technologiach – zgodnie z postanowieniem art. 13 ust. 1 Ustawy KSC – do właściwego CSIRT (lub sektorowego zespołu cyberbezpieczeństwa) w przypadku woli operatora usługi kluczowej dokonania takiego zgłoszenia;
- doradztwo w zakresie przekazanych operatorowi usługi kluczowej zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa oraz przygotowanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń pokontrolnych;

- przygotowanie oszacowania ryzyka wystąpienia incydentu, rozumianego jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo świadczonej usługi kluczowej;
- doradztwo w sprawach związanych z zarządzaniem oszacowanym ryzykiem;
- pomoc w realizacji wynikającego z Ustawy KSC obowiązku operatora usługi kluczowej w zakresie zapewnienia osobom, na rzecz których zadanie publiczne jest realizowane, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, poprzez przygotowanie, a następnie aktualizację, odpowiedniej informacji w postaci broszury dostosowanej do umieszczenia na stronie internetowej operatora usługi kluczowej;
- przeprowadzenie wymaganego przepisem art. 15 ust. 1 Ustawy KSC audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez wyspecjalizowaną kadrę spełniającą wymogi Ustawy KSC oraz Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r., poz. 1999) tj. przynajmniej dwóch audytorów legitymujących się odpowiednimi certyfikatami.
- comiesięczne wykonywanie testów podatności infrastruktury teleinformatycznej z przygotowaniem raportu w języku polskim z opisem podatności oraz rekomendacjami dotyczącymi ich usunięcia.

2. Wsparcie / doradztwo dla Inspektora Ochrony Danych Szpitala poprzez:

- informowanie o obowiązkach spoczywających na jednostce na mocy przepisów o ochronie danych oraz doradztwo w tym zakresie;
- monitorowanie przestrzegania przepisów wewnętrznych, polityk i procedur stosowanych przez jednostkę w zakresie ochrony danych osobowych;
- wykonywanie audytów dotyczących przestrzegania przepisów o ochronie danych osobowych;
- wykonywanie analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych;
- udzielanie jednostce zaleceń co do oceny skutków dla ochrony danych oraz nadzorowanie realizacji zaleceń pokontrolnych;
- aktualizacja dokumentacji tj. rejestru czynności przetwarzania danych osobowych, rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora oraz polityki ochrony danych osobowych – w przypadku zmiany przepisów prawa w w/w zakresie lub na wniosek Inspektora Ochrony Danych;
- doradztwo w przypadku wystąpienia wymaganej na podstawie przepisów prawa współpracy z Prezesem Urzędu Ochrony Danych Osobowych, będącym organem właściwym w sprawach z zakresu ochrony danych osobowych
- wsparcie Inspektora Ochrony Danych w pełnieniu przez niego funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach – w prowadzeniu konsultacji w sprawach dotyczących danych osobowych;
- doradztwo w określeniu zasad i procedur (we współpracy z Działem IT Szpitala) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe; - wsparcie i doradztwo Działu IT w zakresie - adekwatnych do potrzeb i możliwości Szpitala -

rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe;

- wydawanie zaleceń w ramach konsultacji dotyczących wyposażenia jednostki Szpitala w urządzenia do bezpiecznego przechowywania i zabezpieczenia danych osobowych (np. opiniowanie przedstawianych ofert);
- konsultacje w sprawach związanych z przetwarzaniem danych osobowych w systemie informatyczny;
- podejmowanie działań zwiększających świadomość prawną jednostki, jej pracowników i osób wykonujących pracę w oparciu o umowy cywilnoprawne wchodzące w skład kadry pracowniczej, w zakresie przetwarzania i ochrony danych osobowych;
- przeprowadzanie szkoleń pracowników przetwarzających dane osobowe;
- wymagane posiadanie normy na ciągłość działań w obszarze ochrony danych.

2. Termin realizacji zamówienia: na okres 12 miesięcy licząc od dnia podpisania umowy

3. Okres gwarancji: =====

4. Warunki płatności: ryczałtowa, 30 dni od daty otrzymania faktury przez Zamawiającego

5. Inne warunki :

Wykonawca spełni warunek, gdy wykaze, że dysponuje osobami posiadającymi uprawnienia do wykonywania przedmiotu zamówienia tj.

a). co najmniej dwie osoby posiadające odpowiednie umiejętności i uprawnienia:.. legitymujących się certyfikatem uprawniającym do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, określonych 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),

b). osoby wykonującej funkcje Inspektora Ochrony Danych na rzecz podmiotu / podmiotów sektora medycznego (szpitala / szpitali) lub prowadzeniu czynności doradztwa dla Inspektora Ochrony Danych takiego podmiotu / takich podmiotów – minimum 2 lata doświadczenia

Wykonawca spełni warunek, jeżeli wykaze, że posiada:

c). minimum 1 rok doświadczenia (popartego referencjami) w realizacji usługi doradczej w zakresie Krajowego Systemu Cyberbezpieczeństwa oraz przepisów i praktyk dotyczących ochrony danych osobowych świadczonej na rzecz operatora usługi kluczowej sektora medycznego, którego zasoby kadrowe stanowią minimum 1.000 osób (osoby wykonujące prace w oparciu o stosunek pracy lub inne formy zatrudnienia – kontrakty, umowy zlecenia itp.)

d). legitymuje się certyfikatem wdrożonej normy ISO 27001,

e). legitymuje się certyfikatem wdrożonej normy ISO 22301,

f). polisę ubezpieczeniową od odpowiedzialności cywilnej na kwotę minimum 4.000.000 zł. dot. wykonywania audytów i usługi doradczej w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej, wykonywanie u klientów funkcji inspektora danych lub pełnienia funkcji doradczej dla inspektora ochrony danych oraz obejmuje monitorowanie, wdrażanie, nadzorowanie systemu bezpieczeństwa informacji w zakresie przepisów o ochronie danych osobowych, wykonywanie audytów KRI zgodnie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U., poz.526), a w przypadku podmiotów nie realizujących zadań publicznych wykonanie audytów bezpieczeństwa.

O zamówienie mogą ubiegać się wykonawcy nie podlegający wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 15 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Na potwierdzenie braku podstaw do wykluczenia Wykonawca składa oświadczenie – załącznik nr 2 do ZO. W przypadku Wykonawcy wykluczonego z postępowania Zamawiający odrzuci ofertę.

III. DOKUMENTY WYMAGANE OD WYKONAWCY

1. Wypełniony formularz ofertowy (wg załączonego wzoru)- zał 1
2. Wypełnione oświadczenie - Ukraina (wg załączonego wzoru),zał. 2
3. Oświadczenia dotyczące spełnienia warunku z pkt 5 a, b i c
4. Minimum 2 referencje potwierdzające spełnienie warunku z pkt 5 c
5. Certyfikaty normy ISO-27001, i normy ISO- 22301
6. Polisę wraz z dowodem opłacenia składki ubezpieczeniowej- spełnienie warunku z pkt 5 f

Uwaga!

Jeżeli Wykonawca nie złoży wraz z ofertą dokumentów z rozdziału III pkt 2-6 lub złożone dokumenty będą niekompletne lub błędne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie. Brak złożenia formularza ofertowego spowoduje odrzucenie oferty.

7. KRYTERIUM OCENY OFERT

Cena 100%

8. SPOSÓB PRZYGOTOWANIA OFERTY

1. Wykonawca może złożyć wyłącznie jedną ofertę w języku polskim, sporządzonej w formie pisemnej lub elektronicznej lub postaci elektronicznej.
2. Koszty związane z przygotowaniem oferty ponosi składający ofertę. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
3. Złożenie oferty nie powoduje powstania żadnych zobowiązań wobec stron.
4. Oferta Wykonawcy winna spełniać wszystkie wymagania określone w niniejszym zapytaniu , a także zawierać wszystkie żądane dokumenty i załączniki.
5. Zaleca się aby wszystkie strony oferty zostały spięte/zszyte w sposób trwały, zapobiegający możliwości dekompletacji oferty.
6. Złożenie przez wykonawcę fałszywych lub stwierdzających nieprawdę dokumentów lub nierzetelnych oświadczeń mających istotne znaczenie dla prowadzonego postępowania spowoduje odrzucenie oferty.

Dotyczy wyboru dostarczenia oferty drogą pisemną.

1. Oferta oraz wymagane załączniki składane wraz z ofertą wymagają pieczęci i podpisu osób uprawnionych do reprezentowania Wykonawcy w obrocie gospodarczym, zgodnie z aktem rejestracyjnym oraz przepisami prawa.
2. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym

(ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne **pełnomocnictwo** (oryginał lub kopia poświadczona za zgodność z oryginałem przez notariusza).

3. Wszystkie kserokopie dokumentów, oświadczeń winny być poświadczone za zgodność z oryginałem przez wykonawcę lub osobę umocowaną.
4. Poprawki w ofercie muszą być naniesione czytelnie oraz opatrzone podpisem osoby/ osób podpisujących ofertę.
5. W przypadku, gdy oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, Wykonawca winien zastrzec, które spośród zawartych w ofercie informacji nie mogą zostać ujawnione innym uczestnikom postępowania poprzez wydzielenie ich w sposób widoczny i niebudzący wątpliwości, z adnotacją „Tajemnica przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 pzp.

Ofertę należy umieścić w opakowaniu zamkniętym i zaadresowanym do Zamawiającego na adres:

Samodzielny Publiczny Zakład Opieki Zdrowotnej
ul. Młyńska 2 63-700 Krotoszyn
Sekretariat

Zamknięte opakowanie zawierające ofertę Wykonawcy, winno być opisane:

- nazwą i adresem Wykonawcy

Samodzielny Publiczny Zakład Opieki Zdrowotnej
ul. Młyńska 2
63-700 Krotoszyn
Sekretariat

z dopiskiem:

„Zapytanie ofertowe dotyczące:

Wykonanie audytu bezpieczeństwa teleinformatycznego, doradztwo w zakresie cyberbezpieczeństwa oraz ochrony informacji dla operatora usługi kluczowej”

Nie otwierać przed 07.10.2022. r godz. 9.30”.

Zamawiający nie ponosi odpowiedzialności za zdarzenia wynikające z nienależytego oznakowania koperty/opakowania lub braku którejkolwiek z wymaganych informacji.

MIEJSCE I TERMIN ZŁOŻENIA OFERTY

1. Oryginał oferty należy złożyć w siedzibie Zamawiającego ul. Młyńska 2, 63-700 Krotoszyn- sekretariat.
2. Termin składania ofert upływa **w dniu 07.10.2022 r. o godzinie 9.00.** Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone bez otwierania.

Sposób postępowania Wykonawcy w przypadku wyboru formy elektronicznej/postaci elektronicznej

1. Oferta składana jest pod rygorem nieważności w formie elektronicznej (złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
2. Oferta i załączniki do oferty (tj. wymagane oświadczenia i dokumenty) winny być podpisane kwalifikowanym podpisem elektronicznym/profilem zaufanym/podpisem osobistym zgodnie z zasadami jego reprezentacji lub przez jego pełnomocnika.
W przypadku podpisania oferty przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne **pełnomocnictwo** Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez uprawnionego.
3. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 pzp.

Ofertę należy złożyć na:

adres e-mail: donata.lopaczek@spzoz-krotoszyn.pl.

Za ofertę złożoną w terminie Zamawiający uzna przekazaną do dnia 07.10.2022 r. do godz. 09:00. Za datę przekazania oferty przyjmuje się datę jej przekazania na pocztę elektroniczną.

9. WYJAŚNIENIA I MODYFIKACJE ZAPYTANIA OFERTOWEGO

1. Wykonawca może zwrócić się pisemnie (e-mail: donata.lopaczyk@spzoz-krotoszyn.pl), faksem do Zamawiającego o wyjaśnienie treści wszelkich wątpliwości dotyczących zapytania ofertowego oraz sposobu przygotowania i złożenia oferty.
2. Jeżeli wniosek o wyjaśnienie treści zapytania ofertowego dotrze do zamawiającego nie później niż **do końca dnia 29.09.2022 r.** Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie wpłynie po upływie terminu, o którym mowa powyżej Zamawiający będzie miał prawo pozostawić wniosek bez rozpoznania.

10. OSOBA UPOWAŻNIONĄ DO KONTAKTÓW Z WYKONAWCAMI JEST:

w sprawach formalnych:

- Donata Łopaczyk – Specjalista ds. zamówień publicznych, (62) 58 21 222,
e-mail: donata.lopaczyk@spzoz-krotoszyn.pl.

w sprawach merytorycznych:

- Ewelina Brdys – Specjalista ds. Informatyki, (62) 58 21 239,
- Jarosław Ratajek - Specjalista ds. Informatyki (62) 58 21 239,

11. WYBÓR OFERTY, UNIEWAŻNIENIE POSTĘPOWANIA

1. O wyborze najkorzystniejszej oferty Zamawiający powiadomi wybranego wykonawcę pisemnie oraz określi termin podpisania umowy, a w przypadku umieszczenia zapytania ofertowego na stronie internetowej Zamawiający zamieści informację o wyborze oferty na stronie internetowej.
2. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez wyboru oferty, bez podawania przyczyny, na każdym etapie postępowania.

12. ZAŁĄCZNIKI

1. Formularz ofertowy – załącznik nr 1.
2. Oświadczenie – Ukraina – załącznik nr 2

Niniejsze zapytanie ofertowe zatwierdził w dniu 27.09.2022 r

p.o. DYREKTOR
SPZOZ w Krotoszynie
Beata Maj