WYMAGANIA DLA PRZEDMIOTU ZAMÓWIENIA

Zamówienie realizowane jest w ramach Projektu pod nazwą ,,USŁUGĘ DORADCZĄ W ZAKRESIE CYBERBEZPIECZEŃSTWA DLA OPERATORA USŁUGI KLUCZOWEJ WRAZ Z DORADZTWEM W ZAKRESIE OCHRONY DANYCH OSOBOWYCH dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Kępnie. ”

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
systemu zarządzania bezpieczeństwem informacji Zleceniodawcy, wytworzonej zgodnie z wymaganiami normy PN-EN ISO/IEC 27001 i 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 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 wyspecjalizowana 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.

3) Doradztwo Informatyczne obejmujące:

- ścisłą współpracę z Inspektorem Ochrony Danych;
- doradztwa w określeniu zasad i procedur (we współpracy z działem obsługi informatycznej operatora usługi kluczowej) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe;
- wsparcia i doradztwa działu obsługi informatycznej operatora usługi kluczowej w zakresie – adekwatnych do potrzeb i jego możliwości – rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe;
- wydawanie zaleceń w ramach konsultacji dotyczących wyposażenia operatora usługi kluczowej w urządzenia do bezpiecznego przechowywania i zabezpieczenia danych osobowych poprzez opiniowanie przedstawionych przez operatora usługi kluczowej ofert wyposażenia sprzętowego;

- konsultacje działu informatycznego operatora usługi kluczowej w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym.

4) Termin realizacji zamówienia: na okres 12 miesięcy licząc od dnia podpisania umowy

5) Warunki płatności: ryczałtowa, 30 dni od daty otrzymania faktury przez Zamawiającego. Kwota powinna być przedstawiona w formie abonamentu miesięcznego: netto i brutto.

6) Inne warunki :

Wykonawca spełni warunek, gdy wykaże, 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 wykaże, że posiada:

c) minimum 2 lata 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) posiada polisę ubezpieczeniową od odpowiedzialności cywilnej na min. 4.000.000 zł dotyczącą wykonywania audytów i usługi doradczej w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej, wykonywania u klientów funkcji inspektora ochrony danych/pełnienia funkcji doradczej dla inspektora ochrony danych oraz obejmującą 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.