

(120209)

Opis przedmiotu zamówienia

Centrum e-Zdrowia jest jednostką, która od ponad 20 lat dostarcza rozwiązania IT dla systemu ochrony zdrowia. Tworzy usługi cyfrowe, umożliwiające interesariuszom systemu ochrony zdrowia, m.in. pacjentom, pracownikom medycznym i organom administracji publicznej, załatwianie spraw przez Internet. Jednocześnie wspiera pracę profesjonalistów medycznych i umożliwia pacjentom efektywniejsze zarządzanie własnym zdrowiem, dzięki łatwiejszemu dostępowi do danych oraz prostszej komunikacji pomiędzy uczestnikami systemu ochrony zdrowia.

CeZ zarządza ponad 50 centralnymi systemami IT, w tym rejestrami medycznymi, systemami wspomagającymi profilaktykę i leczenie oraz dziedzinowymi systemami teleinformatycznymi. Kluczowym rozwiązaniem dostarczonym przez Centrum jest system e-zdrowie (P1) oraz portfolio cyfrowych produktów dla obywateli i profesjonalistów medycznych, wśród których są:

- aplikacje – Internetowe Konto Pacjenta, mojIKP, gabinet.gov.pl, portal pacjent.gov.pl,
- e-usługi – e-recepta, e-skierowanie, wymiana Elektronicznej Dokumentacji Medycznej, obsługa zdarzeń medycznych, e-rejestracja na szczepienia, Unijny Certyfikat COVID, centralna e-rejestracja.

Z systemów wdrażanych przez CeZ korzystają miliony Polaków, setki tysięcy podmiotów medycznych i farmaceutycznych, a także pracownicy administracyjni. Dostarczane rozwiązania są realizowane zgodnie z potrzebami użytkowników systemu, mają na celu usprawnienie procesów biznesowych. Aby tworzone rozwiązania mogły być w pełni wykorzystywane, Centrum e-Zdrowia realizuje zadania mające na celu wzrost poziomu kompetencji cyfrowych m. in. pracowników medycznych. Jest to nieodzowny element dynamicznie postępującej transformacji cyfrowej ochrony zdrowia. Oprócz budowy systemów i rozwoju usług, CeZ wykorzystuje gromadzone dane w celach analitycznych, wspierając podejmowanie decyzji zarządczych przez instytucje odpowiedzialne za kształtowanie polityki zdrowotnej w Polsce.

Ważnym zadaniem Centrum jest również świadczenie usług z zakresu cyberbezpieczeństwa w obszarze ochrony zdrowia.

W ostatnich latach nastąpił dynamiczny rozwój systemów informacyjnych w ochronie zdrowia. Generują one olbrzymie wolumeny danych. Zbierane dane są cyfrowym śladem po działaniach: wystawieniu czy realizacji recepty, odbytym zdarzeniu medycznym czy sfinansowanym świadczeniu ze środków publicznych. Są również zasobem informacyjnym o potężnym potencjale. Na podstawie posiadanych danych CeZ opracowuje raporty i dashboards, które wspierają Ministerstwo Zdrowia w podejmowaniu decyzji strategicznych, umożliwiają bieżący nadzór nad procesami, w tym kontrolę i działania antyfraudowe.

Gromadzone w systemach utrzymywanych przez CeZ dane stanowią wyzwanie dla organizacji zarówno w kontekście zbierania, przechowywania, przetwarzania, udostępniania jak i zapewnienia ich

bezpieczeństwa. W związku z potrzebą weryfikacji poprawności realizowanych czynności i procesów przetwarzania, niezbędne jest przeprowadzenie zamówienia, które obejmie usługę przeprowadzenia kompleksowego audytu organizacyjno-prawnego w zakresie przetwarzania danych osobowych przez Centrum e-Zdrowia za okres nie dłuższy niż od roku 2020.

1. Celem zamówienia jest zapewnienie zgodności przetwarzania danych osobowych z przepisami prawa oraz zapewnienie bezpieczeństwa tych danych poprzez m.in.:
 - audyt procesu przetwarzania w CeZ danych osobowych, w tym szczególnych kategorii danych osobowych (danych wrażliwych), pod względem zgodności z określonymi normami, standardami i przepisami prawa, w szczególności:
 - Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 poz. 1781);
 - 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);
 - Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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),
 - Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465),
 - Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (Dz. U. z 2017 r. poz. 2247)
 - Analizę podstaw prawnych przetwarzania danych osobowych przez CeZ dla poszczególnych zbiorów danych
 - Analizę podstaw prawnych i zasady łączenia przez CeZ zbiorów w zakresie przetwarzania danych osobowych
 - Analizę podstaw prawnych pozyskiwania przez CeZ danych osobowych w celach ich przetwarzania z innych jednostek np. z NFZ, rejestrów medycznych tworzonych i prowadzonych na podstawie art. 19 Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465),
 - Analizę podstaw prawnych w zakresie przetwarzania przez CeZ danych osobowych w związku z prośbami/poleceniami jednostek zewnętrznych (w tym również poszczególnych Departamentów i jednostek MZ) oraz podstawy udostępniania im danych osobowych. W tym wątku należy uwzględnić wszystkie jednostki/podmioty które kierują zapytania/prośby do CeZ,
 - Analiza podstaw prawnych w zakresie obsługi zgłoszeń w tym poprawa, zmiana, udostępnianie danych osobowych w zakresie e-skierowania, e-recepty, nadawania dostępu do IKP i blokowania dostępu do IKP (dzieci i osoby ubezwłasnowolnione);

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (Dz. U. z 2017 r. poz. 2247)

audyt zgodności procedur CeZ w obszarze przetwarzania danych osobowych, w tym szczególnych kategorii danych osobowych (danych wrażliwych) z przepisami prawa oraz poprawności umocowania CeZ jako podmiotu przetwarzającego dane osobowe w imieniu administratora (art. 4 pkt 8 RODO);

Dla wszystkich zadań audytowych w przypadku identyfikacji braków w CeZ przygotowanie propozycji regulacji normalizujących audytowane zakresy wraz z rekomendacją, według najlepszej praktyki, wzorców dokumentów w zakresie stosownych procedur, instrukcji i regulaminów.

2. Metodologia audytu.

Audyt będzie prowadzony na podstawie dostępnych metod badawczych, w tym minimum:

- analizy obowiązującej w CeZ dokumentacji i procedur;
- wywiadów z pracownikami CeZ;
- stałej współpracy z Zamawiającym:
 - Zamawiający przedstawi swoich przedstawicieli do kontaktu (Zespół Zamawiającego, dalej ZZ).
 - ZZ zastrzega sobie wgląd w prace Audytorów (dalej ZA) na każdym etapie ich pracy.
 - Zamawiający przewiduje robocze spotkania, zgłaszanie wniosków itp. Przedmiotowe spotkania będą odbywać się 2 razy w tygodniu w siedzibie zamawiającego lub online, chyba że ZZ na wniosek ZA lub z własnej inicjatywy zdecyduje inaczej;

3. Przebieg prac i plan prac.

- 3.1 ZZ na spotkaniu rozpoczynającym audyt przekaze ZA m.in.: strukturę organizacyjną, polityki i procedury dotyczące przetwarzania danych osobowych w CeZ;
- 3.2 ZA przedstawi plan prac audytowych, z krótką charakterystyką poszczególnych zadań, potrzebnych dokumentów i innych danych z CeZ, osób do współpracy po stronie CeZ.
- 3.3 ZZ zatwierdzi plan lub zgłosi swoje uwagi, które ZA ma obowiązek uwzględnić.
- 3.4 Plan prac może być zmieniany w trakcie realizacji zamówienia, o ile ZZ wyrazi na to zgodę.
- 3.5 Przedmiotowe zmiany nie stanowią zmiany umowy.
- 3.6 Plan prac musi uwzględniać min. poniższy zakres:
 - harmonogram prac (zgodnie z punkt 5);
 - zapoznanie się ze strukturą organizacyjną CeZ;
 - zapoznanie się z wykonywanymi przez CeZ zadaniami, w których przetwarza dane osobowe;
 - zapoznanie się z dokumentami i procesami dotyczącymi przetwarzania danych osobowych, które posiada CeZ;
 - zapoznanie się ze strukturą danych oraz źródłami ich pochodzenia;
 - weryfikacja/zdefiniowanie obszarów/zagadnień, w których są przetwarzane dane osobowe (obszary mogą być dodawane na dalszych etapach audytu);
 - schemat Raportu - zakres danych, formułę przedstawienia danych.

4. Wynik audytu

Raport stanowiący opracowane rekomendacje w zakresie przedmiotu zamówienia. Dla wszystkich zadań audytowych w przypadku identyfikacji braków w CeZ przygotowanie propozycji

regulacji normalizujących audytowane zakresy wraz z rekomendacją, według najlepszej praktyki, wzorców dokumentów w zakresie stosownych procedur, instrukcji i regulaminów.

Warunkiem odebrania usługi jest przedstawienie Raportu stanowiącego opracowane ustalenia i rekomendacje w zakresie przedmiotu zamówienia.

Raport musi zawierać min.:

- metodologię badań w odniesieniu do poszczególnych obszarów/zagadnień;
- szczegółową analizę wyodrębnionych obszarów/zagadnień z uwzględnieniem: ilości przetwarzania danych, wrażliwości danych, występujących ryzyk, poziomu bezpieczeństwa zapewnionego w CeZ oraz wymaganego przepisami prawa,
- obszary/zagadnienia to min.: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie danych osobowych,
- wskazanie obowiązujących aktów prawnych (krajowych i europejskich) z przypisaniem ich do odpowiednich obszarów/zagadnień,
- wypracowane dobre praktyki dla poszczególnych obszarów/zagadnień,
- uchybienia w działaniu, procesach, dokumentacji, itd., zidentyfikowane dla poszczególnych obszarów/zagadnień,
- ocenę obowiązujących w CeZ dokumentów i procedur w zakresie bezpieczeństwa przetwarzanych danych
- wskazanie koniecznych działań naprawczych systemowych oraz dla poszczególnych obszarów/zagadnień, kierunki dalszego rozwoju w zakresie bezpieczeństwa danych

Raport oraz wszystkie wytworzone dokumenty mają być sporządzony w języku polskim, doręczony w formie elektronicznej, opatrzony bezpiecznym podpisem elektronicznym.

5. Termin realizacji

Zamówienie będzie zrealizowane w terminie 40 dni roboczych.

6. Skład ZA.

Do realizacji zamówienia Wykonawca skieruje Zespół audytowy (ZA) w składzie min.:

Osoba	wymagania
Audytór wiodący	• udokumentowane doświadczenie i uprawnienia Audytora wiodącego, w szczególności w obszarach systemu ochrony zdrowia, • udokumentowane kompetencje i specjalizacja w odpowiednich dziedzinach prawa, w szczególności w zakresie ochrony danych osobowych, w tym szczególnych kategorii danych osobowych (danych wrażliwych)

Zespół audytowy w składzie min. min 2 audytorów z których każdy:	• Posiada wyższe wykształcenie prawnicze; • Prowadził min. 6 audytów dotyczących przetwarzania danych w terminie ostatnich 3 latach przed złożeniem oferty; • prowadził minimum 2 audyty przetwarzania danych wrażliwych lub pracował minimum 24 m-ce na stanowisku dedykowanemu przetwarzaniu danych wrażliwych.
--	---

7. Wymagania dodatkowe

- Wykonawca jest zobowiązany do zachowania w tajemnicy wszelkich informacji i danych dotyczących Zamawiającego, otrzymanych i uzyskanych w związku z wykonaniem zobowiązań wynikających realizacji zamówienia;
- Wykonawca jest zobowiązany do zwrócenia Zamawiającemu wszelkich materiałów (w tym m.in.: przekazanej dokumentacji, nośników danych i innych), w których Wykonawca wszedł w posiadanie podczas realizacji Umowy.