Załącznik nr 2 **SPZOZ/ZAP/366 /2022**

UMOWA

wdrożenia w SP ZOZ w Sanoku przepisów ustawy o krajowym systemie cyberbezpieczeństwa

zwana dalej „**Umową**”, zawarta w dniu … …….. 2022 r. w Sanoku pomiędzy:

Samodzielnym Publicznym Zespołem Opieki Zdrowotnej w Sanoku, adres: ul. 800-lecia 26, 38-500 Sanok, wpisanym do Rejestru Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych zakładów Opieki Zdrowotnej prowadzonego przez Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy – Krajowego Rejestru Sądowego pod numerem KRS: 0000059726, NIP: 6871640438, REGON 3704444345,

reprezentowanym przez Grzegorza Panka - Dyrektora SP ZOZ w Sanoku

zwanym dalej **Szpitalem** lub **Zamawiającym,**

a

……..……

……..,

reprezentowanym(ą) przez: …….. – …….

zwanym dalej **Wykonawcą**,

zwanych dalej łącznie **Stronami**, a z osobna **- Stroną**.

Niniejsza umowa została zawarta w wyniku wyboru oferty Wykonawcy w postępowaniu przeprowadzonym w trybie zapytania ofertowego na podstawie Regulaminu Udzielania Zamówień Publicznych w SP ZOZ w Sanoku dla zamówień o wartości poniżej 130.000,00 zł do których nie mają zastosowania przepisy ustawy z dnia 11.09.2019 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2021 r. poz. 1129 z późn. zm.), zgodnie z art. 2 ust. 1 pkt 1 w/w ustawy.

§ 1
Przedmiot umowy

1. Szpital zamawia a Wykonawca przyjmuje do wykonania usługi polegające na wdrożeniu u Zamawiającego jako Operatora Usługi Kluczowej przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2020 r. poz. 1369 z późn. zm.) – zwanej dalej Ustawą, z podziałem na zadania:
   1) Zadanie 1 - uruchomienie i wdrożenie środków pod kątem poprawy cyberbezpieczeństwa, w tym:
      a) przeprowadzenie szkolenia w formie e-learningowej w zakresie cyberbezpieczeństwa skierowanego do kadry zarządzającej Szpitala oraz jego pracowników w zakresie podstawowej świadomości bezpieczeństwa IT (odrębne szkolenie dla kadry zarządzającej i dla pracowników), obejmującym w szczególności:
         - ochronę przed zaawansowanymi atakami przez pocztę i WWW,
         - tworzenie i zarządzanie polityką haseł i tożsamości,

- zarządzanie ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
- wykonywanie kopii zapasowych oraz tworzenie i utrzymanie polityki ciągłości działania.

2) Zadanie 2 - opracowanie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji, zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz Ustawy, w tym planu odtworzenia po awarii;
3) Zadanie 3 - przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej dwóch audytorów podsiadających certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydane 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;
4) Zadanie 4 - świadczenie obsługi Szpitala jako Operatora Usługi Kluczowej z zakresu cyberbezpieczeństwa zgodnie z Ustawą w okresie 12 miesięcy od przedłożenia wyników audytu, w tym:
   a) wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w imieniu Szpitala;
   b) realizację innych zadań i obowiązków przewidzianych w Ustawie dla Operatorów Usług Kluczowych.

2. Szczegółowy zakres usług objętych przedmiotem umowy (poszczególnymi zadaniami) zawiera załącznik nr 1 - stanowiący integralną część umowy, określający w szczególności:
   1) zasady uruchomienia oraz podjęcia działań wdrożeniowych i konfiguracyjnych dla systemu informacyjnego,
   2) zakres i rodzaj wymaganej do opracowania dokumentacji,
   3) zakres i zasady przeprowadzenia audytu weryfikującego,
   4) zakres usług na świadczenie obsługi Zamawiającego jako Operatora Usługi Kluczowej z zakresu cyberbezpieczeństwa,
   5) terminy wykonania poszczególnych usług objętych umową.

§ 2
Sposób realizacji umowy

1. Wykonawca oświadcza, że spełnia wymogi określone dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, o których mowa w art. 14 ust. 2 Ustawy oraz w przepisach rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2479).
2. Wykonawca oświadcza, że wyznaczona przez Niego osoba, o której mowa w § 1 ust. 1 pkt 4 lit. a umowy, posiada odpowiednie kwalifikacje zawodowe, uprawnienia i zezwolenia przewidziane

w obowiązujących przepisach prawa do pełnienia takiej funkcji, jak również niezbędną wiedzę i doświadczenie.

3. Strony zgodnie postanawiają, że Wykonawca przy wykonywaniu Umowy może posiłkować się poza audytorami wskazanymi w § 1 ust. 1 pkt 3 również innymi pracownikami i współpracownikami Wykonawcy, tj. informatykami i prawnikami, audytorami.
4. Wykonanie części przedmiotu umowy przez inne osoby lub podwykonawcę nie wymaga uprzedniej zgody Szpitala, przy czym Wykonawca odpowiada za działania i zaniechania osób trzecich jak za działania własne.
5. Strony zobowiązują się do wzajemnej współpracy przy realizacji Umowy.
6. Wykonawca zobowiązuje się:

   a) wykonać przedmiot niniejszej umowy z zachowaniem należytej staranności jakiej można wymagać od podmiotu profesjonalnie świadczącego usługi doradcze w zakresie cyberbezpieczeństwa, jak również zgodnie z obowiązującymi w zakresie przedmiotu umowy przepisami;

   b) w przypadku trudności w osiągnięciu kompromisu pomiędzy zaleceniami wydanymi przez Wykonawcę a możliwościami Zamawiającego (w zakresie realizacji Umowy) Strony będą przede wszystkim dążyły do zapewnienia utrzymania ciągłości funkcjonowania Szpitala i poszanowania praw i wolności pacjentów oraz osób zatrudnionych przez Zamawiającego;

   c) w przypadku wystąpienia istotnych z punktu widzenia wykonania usług stanowiących przedmiot umowy problemów, Wykonawca powiadomi o tym fakcie Zamawiającego w terminie 2 dni roboczych, z zachowaniem formy pisemnej lub na adres e-mail Zamawiającego podany w umowie.

§ 3
Zakres obowiązków Szpitala

1. Do obowiązków Szpitala należy zapewnienie wsparcia technicznego dla Wykonawcy w zakresie określonym przez Wykonawcę, a niezbędnym do prawidłowego wykonywania Umowy, tj. udostępnienia Wykonawcy dokumentów źródłowych, pomieszczeń w celu dokonania oględzin, systemów informatycznych przetwarzających dane osobowe i informacji zgodnie z zakresem wskazanym w załączniku nr 1 do niniejszej umowy.
2. Szpital jako Operator Usługi Kluczowej zobowiązuje się przekazać informację do organu właściwego do spraw cyberbezpieczeństwa i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowy zespół cyberbezpieczeństwa o zawarciu niniejszej umowy, w tym danych kontaktowych Wykonawcy, zakresie świadczonej usługi oraz o rozwiązaniu umowy w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.
3. Szpital jako Operator Usługi Kluczowej zobowiązuje się przekazać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV dane osoby, o której mowa w § 1 ust. 1 pkt 4 lit. a, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia zawarcia niniejszej umowy, a także informacje o zmianie tych danych w terminie 14 dni od dnia zmiany.
4. Szpital zobowiązuje się do niezwłocznego informowania Wykonawcy o okolicznościach pozostających w związku z przedmiotem umowy, określonym w załączniku nr 1 do niniejszej umowy, mających istotne znaczenie dla prawidłowego wykonywania przez Wykonawcę obowiązków wynikających z niniejszej umowy.
5. W celu przeprowadzenia przez Wykonawcę szkolenia w zakresie cyberbezpieczeństwa skierowanego do kadry zarządzającej Szpitala lub pracowników Szpitala w zakresie podstawowej świadomości bezpieczeństwa IT, Szpital zapewni lokal i odpowiedni sprzęt umożliwiający przeprowadzenie szkolenia w formie e-learningowej w umówionym przez Strony terminie.

§ 4
Zasady zachowania poufności

1. Strony zapewniają, że zachowają bezterminowo w tajemnicy wszelkie informacje uzyskane w związku z wykonaniem Umowy. Informacje poufne nie będą ujawniane przez żadną ze Stron osobom trzecim, z wyłączeniem osób, którym ujawnienie danych poufnych będzie niezbędne do wykonania postanowień Umowy oraz z wyłączeniem przypadków, gdy ujawnienie danych poufnych będzie wymagane przez przepisy prawa, w szczególności przepisy o dostępie do informacji publicznej.
2. Za informacje poufne strony uważają wszelkie informacje przekazane drugiej stronie w związku i podczas wykonywania Umowy, w szczególności: dotyczące tajemnicy przedsiębiorstwa, dane osobowe lub *know how* którejkolwiek ze Stron.
3. Po rozwiązaniu Umowy każda ze Stron zobowiązana jest niezwłocznie zwrócić drugiej stronie, na jej pisemne żądanie, wszelkie dokumenty i materiały zawierające dane poufne. Rozwiązanie przez strony Umowy nie zwalnia Stron z obowiązku zachowania w tajemnicy danych poufnych.
4. Szpital wyraża zgodę na ujawnianie w celach promocyjnych Wykonawcy faktu współpracy ze Szpitalem w prezentacjach, ofertach, stronach internetowych, publikacjach Wykonawcy w wersji zarówno papierowej, jak i elektronicznej.
5. Szpital wyraża zgodę na posługiwanie się w celach promocyjnych Wykonawcy logiem i nazwą Szpitala w prezentacjach, ofertach, stronach internetowych, publikacjach Wykonawcy w wersji zarówno papierowej, jak i elektronicznej, z oznaczeniem, że Szpital korzysta lub korzystał z usług Wykonawcy.
6. Szpital wyraża zgody, o których mowa w ust. 4 i 5 bezterminowo, bez żadnych ograniczeń terytorialnych, bez obowiązku zapłaty przez Wykonawcę jakiegokolwiek wynagrodzenia.
7. Szpital ma prawo cofnąć udzielone zgody, o których mowa w ust. 4 i 5, jeżeli wypowiedział Umowę z winy Wykonawcy.

§ 5
Prawa autorskie

1. Wykonawca, w ramach wynagrodzenia określonego w Umowie przenosi na Szpital całość autorskich praw majątkowych do dokumentacji systemu zarządzania bezpieczeństwem informacji (dalej zwanej „Utworami") bez jakichkolwiek ograniczeń czasowych, ilościowych i terytorialnych, z chwilą podpisania protokołu odbioru przedmiotu umowy w zakresie zadania 2, na wszystkich znanych polach eksploatacji, a w szczególności w zakresie:
   1) utrwalania i zwielokrotniania Utworów – poprzez wytwarzanie dowolną techniką jego egzemplarzy, w tym techniką drukarską, reprograficzną, zapisu magnetycznego, cyfrową jak również łączącą te techniki, na wszelkich znanych nośnikach,
   2) wprowadzania do obrotu oryginału lub egzemplarzy (kopii) Utworów – w szczególności wprowadzania do obrotu, użyczenia, najmu oryginału albo egzemplarzy,
   3) rozpowszechniania Utworów, w sposób inny niż określony w pkt. 2 powyżej – w szczególności publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie, a także publiczne udostępnianie Utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym, w szczególności za pośrednictwem sieci Internet, udostępniania Utworów na kanałach w mediach społecznościowych i w witrynach Szpitala, w mediach społecznościowych i w witrynach klientów/partnerów biznesowych Szpitala,

4) wykorzystania Utworów w newsletterach, materiałach wewnętrznych i korporacyjnych Szpitala, w tym wydarzeniach / eventach organizowanych przez Szpital oraz w konferencjach prasowych, na pokazach, targach, wystawach i imprezach otwartych i zamkniętych, biletowanych i niebiletowanych - niezależnie od użytego nośnika, a także przy braku fizycznego nośnika, jak również za pomocą dowolnych urządzeń analogowych lub cyfrowych posiadających w szczególności funkcje przechowywania i odczytywania plików audio lub video,
5) wprowadzania do pamięci komputera oraz prywatnych i publicznych sieci komputerowych w tym Internetu, a także rozpowszechniania za pomocą tych sieci;
6) wykorzystania we wszelkich działaniach reklamowych i promocyjnych;
7) prawa do korzystania z dzieł w całości lub z części oraz ich łączenia z innymi dziełami, opracowania poprzez dodanie różnych elementów, uaktualnienie, modyfikację, adaptację, tłumaczenie na różne języki, zmianę barw, okładek, wielkości i treści całości lub ich części;
8) publicznego wystawienia oraz wyświetlenia.

2. Wykonawca udziela Szpitalowi zgody na rozpowszechnianie (w tym w celach komercyjnych) wszelkich wizerunków utrwalonych w ramach Utworów, w zakresie określonym w ust. 1 powyżej, jak również oświadcza, iż uzyskał on zgodę na ich rozpowszechnianie zgodnie z wymogami ustawy z dnia 4.02.1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn. Dz. U. z 2021 r. poz. 1062 z późn. zm.), za co ponosi pełną i osobistą odpowiedzialność.
3. Strony niniejszym uzgadniają, że Zamawiający stanie się właścicielem wszelkich nośników, na których Wykonawca utrwali Utwory, z chwilą dostarczenia tych nośników do Zamawiającego.
4. Wynagrodzenie za przeniesienie majątkowych praw autorskich objęte jest wynagrodzeniem, o którym mowa w § 6 ust. 1 pkt 2 umowy.
5. W ramach wynagrodzenia, o którym mowa w § 6 ust. 1 pkt. 1 umowy, Wykonawca zezwala na wykonywanie przez Zamawiającego zależnych praw autorskich do opracowań, przeróbek utworu i udziela Zamawiającemu wyłącznego prawa zezwalania na wykonywanie zależnych praw autorskich do opracowań, przeróbek utworu oraz prawa do zezwalania na tworzenie opracowań, przeróbek utworu. W związku z wykonywaniem przez Szpital praw zależnych do Utworów oraz zezwalania na wykonywanie praw zależnych do Utworów, Wykonawcy nie będzie przysługiwać dodatkowe wynagrodzenie.
6. W celu uniknięcia wątpliwości, Strony zgodnie stwierdzają, że niniejszy paragraf dotyczy również Utworów w których utrwalone zostały wizerunki lub artystyczne wykonania.
7. Wykonawca zobowiązuje się do niewykonywania nadzoru autorskiego do Utworów. Wykonawca rezygnuje z wyświetlania i umieszczania w/na Utworach swojej nazwy, znaku firmowego i nazwiska twórcy oraz wyraża zgodę na korzystanie z Utworów na podstawie Umowy bez powyższych oznaczeń. Wykonawca zobowiązuje się uzyskać od uprawnionych osób zobowiązanie do niewykonywania autorskich praw osobistych, w szczególności na nieoznaczenie Utworów ich nazwiskami, imionami lub pseudonimami oraz na nieoznaczanie ich jako wykonawców artystycznych wykonań.
8. Wykonawca niniejszym oświadcza, iż przysługują mu autorskie prawa majątkowe do Utworów w zakresie niezbędnym do realizacji niniejszej Umowy i nie są one w żaden sposób ograniczone ani obciążone prawami osób trzecich, oraz są wolne od wad prawnych i fizycznych, a w szczególności, że przeniesienia autorskich praw majatkowych na Szpital oraz korzystania z nich przez Szpital w sposób zgodny z Umową, nie będzie stanowiło naruszenia praw osób trzecich.
9. Wykonawca nie zawarł ani nie zawrze żadnej umowy z podmiotem trzecim, która w jakikolwiek sposób mogłaby kolidować, ograniczyć lub wyłączyć możliwość korzystania przez Szpital z Utworów w sposób zgodny z Umową.

10. W razie skierowania przez osoby trzecie roszczeń wobec Szpitala lub jakichkolwiek podmiotów upoważnionych przez Szpital, w związku z korzystaniem z lub rozpowszechnianiem Utworów w sposób zgodny z Umową, w tym zgodnie z ich przeznaczeniem wynikającym z treści umowy, Wykonawca zobowiązuje się zwolnić Szpital oraz podmioty upoważnione przez Szpital z odpowiedzialności, naprawić wszelkie szkody a także zwrócić Szpitalowi oraz tym podmiotom wszelkie koszty poniesione w związku z takimi roszczeniami, w tym koszty sądowe oraz koszty zastępstwa procesowego.
11. Wszystkie dokumenty i informacje dostarczone Wykonawcy przez Szpital oraz prawa do nich są wyłączną własnością Szpitala i nie mogą być przez Wykonawcę bez zgody Szpitala w jakikolwiek sposób rozporządzane.

§ 6
Wynagrodzenie i sposób zapłaty

1. Wykonawcy przysługuje za realizację Przedmiotu Umowy wynagrodzenie w wysokości:
   1) za wykonanie usług objętych zadaniem 1 określonym w załączniku nr 1 do umowy - …….. zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT, na które składa się:
      a) …… zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT za przeprowadzenie audytu zerowego,
      b) …… zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT za przeprowadzenie szkolenia e-learningowego,
      c) …… zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT za pozostałe usługi objęte zadaniem 1 określonym w załączniku nr 1 do umowy.
   2) za wykonanie usług objętych zadaniem 2 określonym w załączniku nr 1 do umowy - …….. zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT,
   3) za wykonanie usług objętych zadaniem 3 określonym w załączniku nr 1 do umowy - …….. zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT,
   4) za wykonywanie usług objętych zadaniem 4 określonym w załączniku nr 1 do umowy - …….. zł netto (słownie: …….. złotych …./100) plus obowiązująca stawka podatku VAT.
2. Wynagrodzenie określone w ust. 1 pkt. 1-3 jest wynagrodzeniem ryczałtowym, a wynagrodzenie określone w ust. 1 pkt 4 jest wynagrodzeniem miesięcznym dla którego okresem rozliczeniowym jest miesiąc kalendarzowy. Wynagrodzenie, określone w ust. 1 pkt 4, za niepełny okres rozliczeniowy obliczane jest proporcjonalnie do okresu faktycznego wykonywania umowy przez Wykonawcę.
3. Wynagrodzenie Wykonawcy określone w ust. 1 jest stałe i nie podlega waloryzacji. Wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy zawiera wszelkie koszty niezbędne do prawidłowego zrealizowania przez Wykonawcę przedmiotu umowy.
4. W stosunku do części wynagrodzenia, o których mowa w ust. 1 pkt. 1-3 niniejszego paragrafu, podstawą wystawienia faktury VAT przez Wykonawcę jest podpisany przez obie Strony protokół odbioru danej części przedmiotu umowy (poszczególnych zadań), bez zastrzeżeń. Fakturę za usługi objęte zadaniem 4 określonym w załączniku nr 1 do umowy Wykonawca wystawi do 5 dnia miesiąca następującego po miesiącu wykonywania usług objętych tym zadaniem.

5. Zamawiający posiada numer identyfikacyjny NIP 6871640438 i upoważnia Wykonawcę do wystawienia faktury VAT bez pisemnego potwierdzenia odbioru i jej dostarczenia Szpitalowi w formie elektronicznej na adres poczty email: …….
6. Wynagrodzenie, określone w ust. 1 niniejszego paragrafu płatne będzie przelewem na konto Wykonawcy wskazane na fakturze VAT w terminie 30 dni od otrzymania prawidłowo wystawionej faktury VAT wraz z podpisanym przez obie Strony protokołem odbioru danej części przedmiotu umowy bez zastrzeżeń (dotyczy części wynagrodzenia określonych w ust. 1 pkt 1-3).
7. Za datę zapłaty uznaje się dzień obciążenia rachunku bankowego Zamawiającego.
8. W razie opóźnienia płatności przez Zamawiającego Wykonawca ma prawo żądać od Zamawiającego zapłaty odsetek ustawowych za opóźnienie.
9. Wykonawca oświadcza, że nie dokona przeniesienia wierzytelności pieniężnych związanych z realizacją niniejszej umowy na rzecz osób trzecich, bez pisemnej zgody Zamawiającego, oraz nie dokona żadnych innych czynności w wyniku, których doszłoby do zmiany strony umowy.

§ 7
Obowiązywanie umowy

1. Umowa zostaje zawarta na czas określony od dnia …… 2022 r. do dnia …… 2023 r.
2. Szczegółowe terminy realizacji przedmiotu umowy zostały określone w załączniku nr 1 do niniejszej umowy.

§ 8
Odpowiedzialność

1. Wykonawca odpowiada za szkodę wyrządzoną Szpitalowi przy wykonywaniu niniejszej umowy. Odpowiedzialność Wykonawcy jest wyłączona, gdy Szpital nie wprowadził wyraźnych zaleceń Wykonawcy, w szczególności dotyczących wprowadzenia w życie dokumentacji oraz dostosowania systemów informatycznych do wymogów obowiązującego prawa.
2. Wykonawca nie ponosi odpowiedzialności za skutki wynikłe z niezastosowania się Szpitala do zaleceń wydanych przez Wykonawcę.
3. Wykonawca oświadcza, że posiada ubezpieczenie prowadzonej działalności w pełnym zakresie od odpowiedzialności cywilnej kontraktowej w związku z realizacją niniejszej umowy, na sumę ubezpieczenia co najmniej równą łącznej wysokości wynagrodzenia, określonego w § 6 ust. 1 umowy, i zobowiązuje się je utrzymywać przez cały okres obowiązywania umowy. Na każde żądanie Zamawiającego Wykonawca jest obowiązany okazać aktualną opłaconą polisę ubezpieczeniową lub inny dokument potwierdzający posiadanie aktualnego ubezpieczenia.

§ 9
Kary umowne

1. Wykonawca zobowiązuje się do zapłaty Zamawiającemu kar umownych z następujących tytułów i we wskazanych wysokościach:
   1) w przypadku zwłoki w realizacji przedmiotu umowy (poszczególnych zadań) w stosunku do terminów określonych w załączniku nr 1 do umowy, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 0,5% łącznego wynagrodzenia brutto określonego w § 6 ust. 1 pkt. 1-4, za każdy rozpoczęty dzień zwłoki,

2) w przypadku braku reakcji na zgłaszane zapotrzebowanie na konkretne czynności doradcze w ramach obsługi Zamawiającego jako Operatora Usługi Kluczowej w zakresie cyberbezpieczeństwa w terminie do godz. 14:00 następnego dnia roboczego od zgłoszenia, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 0,6% łącznego wynagrodzenia brutto określonego w § 6 ust. 1 pkt. 1-4, za każdy rozpoczęty dzień zwłoki.

2. O nałożonych karach, o których mowa w ust. 1 Zamawiający powiadomi na piśmie Wykonawcę.
3. Łączna wysokość kar umownych nie może przekroczyć 50% łącznej kwoty wynagrodzenia, o której mowa w § 6 ust. 1 pkt 1-4 umowy.
4. Zamawiający zastrzega sobie prawo potrącenia kary umownej z wierzytelnością wynikającą z faktury wystawionej przez Wykonawcę w ramach niniejszej umowy, bez oddzielnego wezwania do zapłaty, na co Wykonawca wyraża zgodę. W związku z dokonanym potrąceniem, Szpital wystawi i prześle Wykonawcy notę obciążeniową.
5. Zamawiający może dochodzić na zasadach ogólnych odszkodowania w zakresie w jakim szkoda Zamawiającego przewyższa wysokość zastrzeżonych kar umownych, jak również w przypadkach dla których kara umowna nie została zastrzeżona.
6. Kary umowne nie zostaną naliczone wyłącznie w przypadku, gdy niewykonanie lub nienależyte wykonanie zobowiązania nastąpiło na skutek siły wyższej.
7. Żadna ze Stron nie będzie ponosić odpowiedzialności za opóźnienia spowodowane siłą wyższą. Przez siłę wyższą rozumie się wszelkie nieprzewidziane zdarzenia powstałe poza kontrolą Stron, których nie mogły przewidzieć ani im zapobiec, pomimo dołożenia wszelkich starań, takie jak: katastrofalne działanie sił przyrody, wojna, strajki generalne, ataki terrorystyczne, akty władzy publicznej, którym nie może przeciwstawić się jednostka itp. W przypadku siły wyższej Strona dotknięta jej działaniem niezwłocznie poinformuje pisemnie drugą Stronę i Strony, uzgodnią tryb dalszego postępowania.

§ 10
Ochrona danych osobowych

1. Strony zgodnie potwierdzają, iż będą przestrzegać obowiązujących przepisów w zakresie ochrony danych osobowych, w tym 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, dalej jako „RODO”), w odniesieniu do wszystkich danych osobowych udostępnionych w ramach realizacji niniejszej Umowy.
2. Strony zgodnie potwierdzają, że dane osobowe osób fizycznych reprezentujących, upoważnionych przez nich do określonych czynności w związku z wykonywaniem niniejszej Umowy albo osób kontaktowych związanych z wykonywaniem niniejszej Umowy będą przetwarzały jako dane niezbędne do celów wynikających z ich prawnie uzasadnionych interesów jako administratorów, związanych z odpowiednim wykonywaniem niniejszej Umowy oraz że są upoważnione do udostępnienia tych danych drugiej Stronie Umowy w oparciu o stosowną przesłankę wynikającą z RODO.
3. Strony zobowiązane są do poinformowania osób, o których mowa w ust. 2, o tym że druga Strona niniejszej Umowy będzie administratorem ich danych osobowych i będzie te dane przetwarzać w celach o których mowa w ust. 2 powyżej, tak aby druga Strona mogła powołać się na art. 14 ust. 5 lit. a) RODO.
4. Szpital powierza Wykonawcy przetwarzanie danych osobowych w imieniu Zamawiającego, na zasadach określonych w Umowie powierzenia przetwarzania danych osobowych, stanowiącej załącznik nr 2 do niniejszej umowy oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w RODO.

5. Wykonawca oświadcza że Zamawiający na podstawie art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO), poinformował go, że:
   1) administratorem danych osobowych Wykonawcy jest Samodzielny Publiczny Zespół Opieki Zdrowotnej w Sanoku, adres: ul. 800-lecia 26, 38-500 Sanok;
   2) administrator wyznaczył Inspektora Ochrony Danych, z którym Wykonawca może się kontaktować w sprawach przetwarzania danych osobowych za pośrednictwem poczty elektronicznej: rodo@zozsanok.pl
   3) administrator będzie przetwarzał dane osobowe Wykonawcy na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z realizacją niniejszej umowy;
   4) dane osobowe Wykonawcy mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także podmiotom, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);
   5) administrator nie zamierza przekazywać danych osobowych Wykonawcy do państwa trzeciego lub organizacji międzynarodowej;
   6) Wykonawca ma prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.
6. Wykonawca oświadcza również, że Zamawiający na podstawie art. 13 ust. 2 Ogólnego Rozporządzenia o Ochronie Danych (RODO), poinformował go, że:
   1) dane osobowe Wykonawcy będą przetwarzane przez okres przedawnienia roszczeń wynikających z umowy określony w Kodeksie cywilnym albo w przypadku zamówień realizowanych w ramach projektów (np. współfinansowanych ze środków Unii Europejskiej) przez okres wskazany w wytycznych w zakresie kwalifikowalności wydatków;
   2) Wykonawcy przysługuje prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;
   3) podanie danych osobowych Wykonawcy jest dobrowolne, jednakże niezbędne do realizacji ww. celu. Konsekwencje niepodania danych określają przepisy odrębne;
   4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o dane osobowe Wykonawcy.

§ 11
Osoby kontaktowe

1. W sprawach związanych z realizacją umowy osobami kontaktowymi będą:
   1) po stronie Wykonawcy:
      ……, tel. …….., e-mail: ……
   2) po stronie Szpitala:
      ……., tel. …….., e-mail: ……
2. Zmiana wymienionych w ust. 1 przedstawicieli Stron lub ich danych kontaktowych nie wymaga zmiany Umowy i następuje w trybie powiadomienia pisemnego drugiej Strony Umowy.

§ 12
Rozwiązanie i odstąpienie od umowy

1. Zamawiający zastrzega sobie prawo rozwiązania umowy w przypadkach niewykonania lub nienależytego wykonania umowy, po uprzednim wezwaniu Wykonawcy do należytego wykonania

i wyznaczeniu w tym celu dodatkowego minimum 7 dniowego terminu. Rozwiązanie umowy następuje w trybie wypowiedzenia umowy ze skutkiem natychmiastowym.

2. Rozwiązanie umowy za wypowiedzeniem wymaga zachowania formy pisemnej i wskazania przyczyny. O dacie wypowiedzenia decyduje data doręczenia drugiej stronie.
3. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie Zmawiającego, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.

§ 13
Postanowienia końcowe

1. Zmiany Umowy mogą być dokonane tylko w formie pisemnej pod rygorem nieważności.
2. Sądem właściwym do rozstrzygania sporów powstałych w związku z realizacją Umowy będzie Sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych w Umowie należy stosować odpowiednio przepisy Kodeksu cywilnego, Ustawy i innych przepisów prawa powszechnie obowiązującego związanego z przedmiotem umowy.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

_____ _____

Szpital Wykonawca

Załączniki:

1. Opis przedmiotu zamówienia.
2. Umowa powierzenia przetwarzania danych osobowych.

Załącznik nr 1 do umowy – Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie usługi polegającej na opracowaniu i wdrożeniu systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym w SPZOZ w Sanoku jako operatora usługi kluczowej i jego dostosowania do wymogów Ustawy z dnia 05.07.2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 poz. 1369 z późn. zm. – zwana dalej Ustawą) wraz z powiązanymi aktami wykonawczymi, w szczególności w zakresie wymogów, jakie operatorzy usług kluczowych zobowiązani są spełnić w terminie 3 miesięcy od doręczenia decyzji o uznaniu za operatora usługi kluczowej.

Zakres zadań:

1. Uruchomienie i wdrożenie środków pod kątem poprawy cyberbezpieczeństwa.

Wdrożenie systemu bezpieczeństwa informacji powinno poprzedzić zbadanie systemów informatycznych w Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Sanoku pod w tym zakresie (audyt zerowy). Jego celem jest przeprowadzenie oceny czy wewnętrzne procesy i zastosowane środki techniczne sprzyjają bezpiecznemu przetwarzaniu danych w systemach pod kątem zgodności z Ustawą.

Warunki i zakres przeprowadzenia audytu zerowego w zakresie sprawdzenia bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z wymaganiami Ustawy:

a) Analiza procesów przetwarzania danych wraz z analizą stanu zabezpieczeń systemowych.
b) Identyfikacja informacji i jej klasyfikacja.
c) Inwentaryzacja zasobów infrastruktury teleinformatycznej, oprogramowania i obszarów bezpiecznych.
d) Identyfikacja i analiza podatności systemów wspomagających świadczenie usługi kluczowej.
   Wynikiem analizy musi być pełna lista przeskanowanych pod kątem podatności, systemów zawierająca informacje obejmujące: skanowany system operacyjny, uruchomione na nim usługi, otwarte porty komunikacyjne, listę wykrytych podatności oraz wytyczne dotyczące sposobu usunięcia wykrytych podatności. W celu wykonania powyższych czynności, Wykonawca zobowiązany jest do zapewnienia odpowiedniej licencji na system skanujący.

Zamawiający wymaga, aby przedmiotowa analiza i ocena cyberbezpieczeństwa realizowana była w oparciu o normę PN ISO/IEC 27001.

e) Analiza bezpieczeństwa fizycznego i środowiskowego dla zabezpieczenia realizacji usługi kluczowej.
f) Zarządzanie: ryzykiem, incydentem, podatnościami, środkami technicznymi i organizacyjnymi, systemem monitorowania w trybie ciągłym.
g) Inwentaryzacja procedur.
h) Bezpieczeństwo i ciągłość dostaw i usług od których zależy świadczenie usługi kluczowej.
i) Przegląd dokumentacji związanej z cyberbezpieczeństwem.
j) Zidentyfikowaniu wszelkich niezgodności i wdrożenie działań naprawczych.

Audyt będzie się opierać na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby w wybranych lokalizacjach Zamawiającego oraz z wykorzystaniem zdalnego dostępu. Ponadto analiza oparta będzie o wywiad i oświadczenia wskazanych przez Zamawiającego osób.

Audyt bezpieczeństwa, może być przeprowadzony przez:

- jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 5 z późn. zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
- co najmniej dwóch audytorów posiadających:
  - certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
  - co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
  - co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
- Wykonawca przedstawi w sposób udokumentowany doświadczenie realizacji projektów z zakresu Systemów Bezpieczeństwa Informacji (audyt lub wdrożenie) w jednostkach medycznych w okresie 3 lat.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);

- 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, w zakresie certyfikacji osób;
- 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;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą w/w certyfikatów.

Wnioski wypływające z audytu powinny wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Wynikiem audytu będzie sporządzenie przez Wykonawcę raportu określającego konieczne działania, a także zawierającego specyfikację rozwiązań sprzętowych oraz programowych wraz z kompleksową informacją na temat ich wdrożenia i wykorzystania u Zamawiającego celem osiągnięcia zgodności z wymaganiami Ustawy.

Powyższe wytyczne, rekomendacje oraz opisy techniczne rozwiązań (wraz z szacunkową wyceną) dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, powinny obejmować m.in.:

- utrzymania i bezpiecznej eksploatacji systemu informacyjnego,
- bezpieczeństwa fizycznego i środowiskowego, uwzględniając kontrolę dostępu,
- bezpieczeństwa oraz ciągłości dostaw i usług, od których zależy świadczenie usługi kluczowej,
- wdrażania, dokumentowania i utrzymywania planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
- objęcia systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, systemem monitorowania w trybie ciągłym,

- wdrożenia odpowiednich środków organizacyjnych wymaganych ustawą w celu świadczenia usługi kluczowej,
- wdrożenia wymaganej ustawą dokumentacji systemu cyberbezpieczeństwa.

Uruchomienie i działania po wdrożeniu środków stanowiących rekomendacje wynikające z przeprowadzonego audytu zerowego:

a) Uruchomienie i wdrożenie programu systematycznej analizy ryzyka i zarządzania ryzykiem.
b) Uruchomienie systemu zarządzania incydentami bezpieczeństwa, pozwalający m.in. na zgłaszanie poważnych incydentów do krajowego zespołu CSIRT w czasie nieprzekraczającym 24 godzin od ich wykrycia.
c) Wdrożenie programu edukacji użytkowników usługi kluczowej w zakresie cyberbezpieczeństwa, w tym przeprowadzenie szkolenia w formie e-learningowej w zakresie cyberbezpieczeństwa skierowanego do kadry zarządzającej Szpitala oraz jego pracowników w zakresie podstawowej świadomości bezpieczeństwa IT (odrębne szkolenie dla kadry zarządzającej i dla pracowników), obejmującym w szczególności:
   - ochronę przed zaawansowanymi atakami przez pocztę i WWW,
   - tworzenie i zarządzanie polityką haseł i tożsamości,
   - zarządzanie ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
   - wykonywanie kopii zapasowych oraz tworzenie i utrzymanie polityki ciągłości działania.
d) Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych.
e) Wdrożenie bezpieczeństwa fizycznego i środowiskowego, uwzględniającego kontrolę dostępu.
f) Wdrożenie bezpieczeństwa i ciągłości dostaw usług, od których zależy świadczenie usługi kluczowej.
g) Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym.
h) Uruchomienie systemu do zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Wykonawca zapewni wszelką pomoc, o którą zwróci się Zamawiający w zakresie wdrożenia środków zaradczych, instalacji i konfiguracji oprogramowania oraz udzieli niezbędnego wsparcia.

2. **Opracowanie i wdrożenie dokumentacji systemu zarządzania bezpieczeństwem informacji**, w tym:

a) Opracowanie i zapewnienie aktualności dokumentacji dotyczącej cyberbezpieczeństwa systemów informatycznych oraz bezpieczeństwa przetwarzania informacji wykorzystywanych do świadczenia usługi kluczowej.
b) Opracowanie Polityki Bezpieczeństwa Informacji.
c) Rejestr zdarzeń i incydentów.

Wykonawca w ramach wynagrodzenia zobowiązany jest do przeniesienia na Zamawiającego autorskich praw majątkowych do wszelkiej opracowanej i wytworzonej dokumentacji systemu zarządzania bezpieczeństwem informacji.

3. Przeprowadzenie audytu weryfikującego.

Warunki i zakres audytu zgodny z pkt. 1.
Celem audytu jest sprawdzenie skuteczności i efektywności działań korygujących oraz ewentualne wykazanie przez Zamawiającego podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności z punktów 1-2.

Osoby tworzące uczestniczące w audycie weryfikującym i bezpośrednio zaangażowane w kontrolę zgodności muszą pozostać obiektywne i niezależne. Oznacza, to iż działając w ramach międzynarodowych standardów audytu nie mogą dokonywać oceny obszaru, za który były odpowiedzialne lub prowadziły czynności doradcze.

Wobec tego Wykonawca zobowiązany jest do spełnienia powyższego warunku poprzez zapewnienie odrębnego zespołu audytowego lub umowę podwykonawstwa.

Wszystkie osoby zaangażowane w badanie składają oświadczenie o braku konfliktu interesów, w szczególności w terminie ostatnich 24 miesięcy nie wykonywały osobiście prac doradczych, projektowych, architektonicznych lub implementacyjnych na rzecz audytowanego podmiotu w zakresie audytowanej usługi kluczowej.

4. Usługa świadczenia obsługi jednostki jako operatora usługi kluczowej z zakresu cyberbezpieczeństwa zgodnie z Ustawą w okresie 12 m-cy od przedłożenia wyników audytu weryfikującego.

a) Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.
b) Utrzymanie i bezpieczną eksploatację systemu informacyjnego.

c) Wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji.
d) Zarządzanie incydentami oraz zapewnienie dostępu do rejestrowanych incydentach właściwemu organowi.
e) Klasyfikuje incydenty.
f) Zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT.
g) Współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe.
h) Usuwa podatności oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.
i) Nadzór nad mechanizmami zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.
j) Dbałość o aktualizację oprogramowania.
k) Stosowanie środków zapewniających ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym.
l) Niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.
m) Aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

5. Terminy

L.p.	Zadania	Okres
1	Uruchomienie i wdrożenie środków pod kątem poprawy cyberbezpieczeństwa - w tym ukończenie audytu zerowego	do 31.08.2022 do 22.07.2022
2	Opracowanie i wdrożenie dokumentacji systemu zarządzania bezpieczeństwem informacji	do 09.09.2022
3	Przeprowadzenie audytu weryfikującego	do 15.09.2022
4	Usługa świadczenia obsługi jednostki jako Operatora Usługi Kluczowej z zakresu cyberbezpieczeństwa zgodnie z Ustawą w okresie 12 m-cy od przedłożenia wyników audytu weryfikującego	od 01.10.2022 do 30.09.2023

Załącznik nr 2 do umowy – umowa powierzenia przetwarzania danych osobowych

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Niniejsza umowa została zawarta w Sanoku w dniu ……. r. pomiędzy:

Samodzielnym Publicznym Zespołem Opieki Zdrowotnej w Sanoku, adres: ul. 800-lecia 26 38-500 Sanok, wpisanym do Rejestru Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych zakładów Opieki Zdrowotnej prowadzonego przez Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy – Krajowego Rejestru Sądowego pod numerem KRS: 0000059726, NIP: 6871640438, REGON 3704444345,

reprezentowanym przez Grzegorza Panka - Dyrektora SP ZOZ w Sanoku

zwanym dalej „**Administratorem**”

a

……..……

……..,

reprezentowanym(ą) przez: …….. – …….

zwanym dalej „**Podmiotem Przetwarzającym**”

zwanych dalej łącznie „**Stronami**”, a z osobna „**Stroną**”.

Zważywszy, że:

1. Administrator jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 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, zwanego dalej „RODO”, wskazanych w załączniku nr 1 do umowy.
2. Administrator zamierza powierzyć Podmiotowi Przetwarzającemu przetwarzanie danych osobowych, a Podmiot Przetwarzający zamierza przyjąć powierzone mu dane osobowe do przetwarzania w imieniu Administratora, zgodnie z umową oraz z przepisami regulującymi przetwarzanie danych osobowych, wiążącymi Podmiot Przetwarzający i Administratora.

Strony postanowiły, co następuje:

§ 1
Przedmiot umowy

1. Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych w imieniu Administratora, na zasadach określonych w Umowie oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w RODO.
2. Rodzaj danych osobowych, kategorie osób, których dotyczą dane osobowe, jak również przedmiot, czas trwania, charakter i cel przetwarzania danych osobowych są wskazane w załączniku nr 1 do umowy.

3. Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.

§ 2
Oświadczenie Podmiotu Przetwarzającego

Podmiot Przetwarzający oświadcza, że:

a) wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą dane osobowe; oraz
b) dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającymi prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonych w umowie.

§ 3
Przetwarzanie danych osobowych

1. Z zastrzeżeniem ust. 2, przetwarzanie danych osobowych przez Podmiot Przetwarzający może następować wyłącznie w przypadkach wynikających z Umowy lub na podstawie odrębnych zleceń Administratora, wyrażonych w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej).
2. Podmiot Przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku Podmiot Przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.
3. Przetwarzanie danych osobowych przez Podmiot Przetwarzający jest ograniczone do celu i zakresu wskazanych w załączniku nr 1 do umowy.
4. Podmiot Przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, zawierający informacje wymagane przez obowiązujące przepisy, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
5. Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
6. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych Podmiot Przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.
7. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot Przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
8. Podmiot Przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
   a) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
   b) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;

c) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2; oraz
d) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Podmiot Przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.

9. Podmiot Przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych, o których mowa w ust. 8 lit. a).

§ 4
Dalsze powierzenia przetwarzania

1. Podmiot Przetwarzający ma prawo korzystać z podwykonawców przy przetwarzaniu danych osobowych (dalsze powierzenie przetwarzania), pod warunkiem, że przed powierzeniem podwykonawcy przetwarzania danych osobowych:
   a) uzyska na to zgodę Administratora, wyrażoną w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej);
   b) zawrze z podwykonawcą umowę powierzenia przetwarzania danych osobowych na warunkach nie gorszych niż warunki umowy;
   c) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów.
2. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wypełnienie obowiązków podwykonawcy.
3. Wykaz podwykonawców, z których Podmiot Przetwarzający korzysta w dniu zawarcia umowy, i co do których Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych, stanowi załącznik nr 2 do umowy.

§ 5
Bezpieczeństwo danych osobowych

1. Podmiot Przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.

2. Podmiot Przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa, i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne, tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.

3. Podmiot Przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.

4. Podmiot Przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:

a) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
b) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.

5. Podmiot Przetwarzający niezwłocznie – w każdym wypadku nie później niż w ciągu 24 godzin od wykrycia – informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi Przetwarzającemu informacje na temat naruszenia, w szczególności:
   a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) możliwe konsekwencje naruszenia ochrony danych osobowych; oraz
   d) środki zastosowane lub proponowane przez Podmiot Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Podmiot Przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.
7. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.

§ 6
Prawo do kontroli

1. Administrator ma prawo kontrolowania sposobu wypełniania przez Podmiot Przetwarzający jego obowiązków określonych w umowie lub w obowiązujących przepisach. W szczególności Administrator może żądać udostępnienia określonych informacji lub dokumentów oraz może przeprowadzać – samodzielnie lub przez upoważnionego przez Administratora pracownika lub współpracownika – audyty, w tym inspekcje w miejscu przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. Podmiot Przetwarzający ma obowiązek współpracować z Administratorem lub upoważnionym przez Administratora pracownikiem lub współpracownikiem w czasie przeprowadzanej kontroli, w sposób umożliwiający Administratorowi weryfikację prawidłowej realizacji obowiązków Podmiotu Przetwarzającego.

§ 7
Rozwiązanie umowy

1. Umowa wchodzi w życie z dniem podpisania i zostaje zawarta na czas określony do dnia rozwiązania lub wygaśnięcia ostatniej z umów łączących Strony, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. W przypadku stwierdzenia naruszenia przez Podmiot Przetwarzający obowiązków wynikających z umowy, Administrator ma prawo rozwiązać wszystkie umowy zawarte z Podmiotem Przetwarzającym, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający, ze skutkiem natychmiastowym.
3. Najpóźniej w dniu rozwiązania umowy Podmiot Przetwarzający ma obowiązek:

a) usunąć wszelkie dane osobowe; albo
b) zwrócić Administratorowi wszelkie nośniki zawierające dane osobowe oraz usunąć wszelkie istniejące kopie danych osobowych, chyba że obowiązujące przepisy wymagają od niego dalszego przechowywania części lub całości danych osobowych,
c) zależnie od wyboru Administratora, zakomunikowanego Podmiotowi Przetwarzającemu w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej) co najmniej na 7 dni przed terminem rozwiązania Umowy.

4. W przypadku rozwiązania Umowy w trybie ust. 2 wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
5. Czynności wskazane w ust. 3 zostaną wykazane w pisemnym protokole, podpisanym przez przedstawiciela Podmiotu Przetwarzającego i dostarczonym Administratorowi w terminie 7 dni od dokonania wskazanych w nim czynności.

§ 8
Postanowienia końcowe

1. Podmiotowi Przetwarzającemu nie przysługuje wynagrodzenie za wykonywanie Umowy.
2. Umowa stanowi całość porozumienia pomiędzy Stronami i zastępuje w całości uprzednie lub równoczesne uzgodnienia poczynione przez Strony (w formie pisemnej lub ustnej) w przedmiocie regulowanym postanowieniami niniejszej Umowy.
3. Załączniki do Umowy stanowią jej integralną część.
4. Wszelkie spory między Stronami będą rozwiązywane na zasadzie polubownych negocjacji. W przypadku nieosiągnięcia przez Strony porozumienia, spór zostanie przekazany do rozstrzygnięcia sądowi powszechnemu właściwemu dla siedziby Administratora.
5. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.

Administrator: Podmiot Przetwarzający:

_____ _____

Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych – Dane osobowe

Rodzaje danych osobowych (np. imię, nazwisko, adres, numer PESEL, numer telefonu, e-mail, adres IP, dane o stanie zdrowia)	Zwykłe dane identyfikacyjne takie jak: imię i nazwisko; wizerunek; data urodzenia; miejsce urodzenia; miejsce pracy; płeć; obywatelstwo; adres zamieszkania; miejsce zameldowania; adres do korespondencji; numer telefonu; adres poczty elektronicznej;
Kategorie osób, których dane osobowe dotyczą (np. pracownicy, dostawcy, pacjenci, kontrahenci, klienci)	pracownicy i współpracownicy, w tym byli pracownicy i współpracownicy oraz członkowie ich rodzin; potencjalni pracownicy i współpracownicy; potencjalni dostawcy oraz ich pracownicy i współpracownicy; dostawcy oraz ich pracownicy i współpracownicy; osoby składające skargi, wnioski i petycje; osoby wnioskujące o udostępnienie informacji publicznej; osoby korespondujące z administratorem; wierzyciele i dłużnicy; pacjenci i byli pacjenci
Zakres przetwarzania danych osobowych (czynności dokonywane na powierzonych danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, udostępnianie, zmienianie, usuwanie)	zbieranie, utrwalanie, organizowanie, przechowywanie, pobieranie, przeglądanie, usuwanie
Charakter przetwarzania (np. systematyczny/sporadyczny)	systematyczny
Cel przetwarzania (np. wykonanie umowy z dnia…)	Realizacja umowy o współpracy w zakresie wdrożenia ustawy o krajowym systemie cyberbezpieczeństwa z dnia …….
Czas przetwarzania (np. *okres obowiązywania umowy z dnia…)*	Na czas trwania umowy o współpracy w zakresie wdrożenia ustawy o krajowym systemie cyberbezpieczeństwa z dnia …….

Załącznik nr 2 do umowy powierzenia przetwarzania danych osobowych – Podwykonawcy zatwierdzeni przez Administratora

Lp.	Nazwa	Adres	NIP
1.			
2.			
3.			