Wojewódzkie Wielospecjalistyczne Centrum Onkologii
i Traumatologii im. M. Kopernika w Łodzi
nazwa komórki: ***Dział Informatyki***
tel. 042 689 5409, 5868
e-mail: ***postepowania-it@kopernik.lodz.pl***

Łódź, dnia 17.03.2026r.

Nr sprawy: EI.273.10.III.2026

ZAPYTANIE OFERTOWE [ZO]

DOTYCZY: Postępowania o udzielenie zamówienia publicznego o wartości nie przekraczającej **170 000,00 zł netto**

na świadczenie usługi wsparcia technicznego
w zakresie utrzymania i rozwoju Systemu Portal Pacjenta
w Wojewódzkim Wielospecjalistycznym Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi
prowadzone zgodnie z art. 2 ust.1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych [tj. Dz.U. z 2024 r. poz. 1320.ze zm.]

KIEROWNIK
Działu Informatyki
inż. Robert Rożniakowski
.....
podpis

I. ZAMAWIAJĄCY

Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi
Dział Informatyki
Ul. Pabianicka 62
93-513 Łódź
e-mail: **postepowania-it@kopernik.lodz.pl**
strona prowadzonego postępowania: kopernik.lodz.pl/zamowienia-do-170-000-zl/

II. PODSTAWA PRAWNA.

Postępowanie prowadzone jest zgodnie z art. 2 ust.1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

III. PRZEDMIOT ZAMÓWIENIA

Przedmiot zamówienia stanowi świadczenie usługi wsparcia technicznego w zakresie utrzymania i rozwoju Systemu Portal Pacjenta w Wojewódzkim Wielospecjalistycznym Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi - szczegółowy Opis przedmiotu zamówienia zawiera załącznik nr 3 - Wzór umowy

IV. TERMIN REALIZACJI.

1. Termin realizacji **24 miesiące** od dnia udzielenia zamówienia (podpisania umowy).

V. ZAPYTANIA DO ZAMAWIAJĄCEGO.

1. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści zapytania ofertowego.
2. W przypadku zapytań prosimy kontaktować się z Działem Informatyki pod adresem e-mail: postepowania-it@kopernik.lodz.pl
3. Pytania można przesłać najpóźniej **48 godzin** przed upływem terminu składania ofert.
4. W przypadku gdy wniosek o wyjaśnienie treści ZO nie wpłynął w terminie, zamawiający nie ma obowiązku udzielania wyjaśnień .
5. Treść zapytań wraz z wyjaśnieniami zamawiający udostępni na stronie internetowej prowadzonego postępowania.

VI. WYMAGANE DOKUMENTY

1. Oferta winna zawierać następujące dokumenty w **formie podpisanych skanów lub dokumentów podpisanych kwalifikowanym podpisem elektronicznym, lub podpisem zaufanym, lub podpisem osobistym**:
   a) Wypełniony **Formularz ofertowy -Załącznik nr 1**;
   b) **Oświadczenie** wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia uwzględniające przesłanki wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie
   c) Odpis z Krajowego Rejestru Sądowego lub aktualny wypis z CEIDG;
   d) Pełnomocnictwo do reprezentacji wykonawcy, jeżeli uprawnienie do podpisania oferty i poświadczenia dokumentów za zgodność z oryginałem nie wynika z KRS lub CEIDG;

VII. SPOSÓB I TERMIN ZŁOŻENIA I OTWARCIA OFERTY

1. Ofertę, wraz z wymaganymi załącznikami należy złożyć przed terminem składania ofert.
2. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
3. Ofertę, za pomocą poczty elektronicznej, wraz z wymaganymi dokumentami, zawierającą dane Wykonawcy należy wysłać na adres mailowy: postepowania-it@kopernik.lodz.pl do dnia **24.03.2026 .do godz.:13.00.**
4. Zamawiający ma prawo zmiany terminu złożenia oferty.
5. Zamawiający poinformuje o zmianie terminu składania na stronie internetowej prowadzonego postepowania.
6. Termin związania ofertą wynosi **45 dni** od dnia jej otrzymania przez Zamawiającego.
7. Zamawiający ma prawo zwrócić się do wykonawcy o wyrażenie zgody na przedłużenie terminu związania ofertą o kolejne 30 dni.
8. Jeżeli termin związania ofertą upłynie przed wyborem oferty, Zamawiający może wezwać Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, zgody na wybór jego oferty. W przypadku braku zgody, oferta Wykonawcy podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.
9. Wykonawca może złożyć tylko jedną ofertę.
10. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

11. Otwarcie ofert jest niejawne.
12. Wykonawcy składającemu oferty nie przysługują środki ochrony prawnej w postaci odwołania od czynności Zamawiającego.
13. Zamawiający udzieli zamówienia Wykonawcy, którego oferta:
    a) odpowiadać będzie wymaganiom określonym w zapytaniu ofertowym,
    b) zostanie uznana za najkorzystniejszą w oparciu o podane kryteria oceny ofert
14. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że zostały złożone oferty przedstawiające taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
15. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera ofertę z najniższą ceną.
16. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa wyżej, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.
17. Wykonawcy, składając oferty dodatkowe, nie mogą oferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
18. Ocenie będą podlegać wyłącznie oferty niepodlegające odrzuceniu.

VIII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT.

1. Kryteria oceny ofert: **cena 100 %**

IX. BADANIE I OCENA OFERT.

1. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert oraz innych składanych dokumentów lub oświadczeń.
2. Zamawiający może poprawić w ofercie:
   1) oczywiste omyłki pisarskie,
   2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   3) inne omyłki polegające na niezgodności oferty z warunkami zamówienia,
   - zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
3. W przypadku, o którym mowa w ust. 2 pkt 3), zamawiający wyznaczy wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.
4. Zamawiający zastrzega sobie prawo wezwania do wyjaśnienia ceny złożonej oferty, jeżeli będzie ona wzbudzała wątpliwości (w szczególności w przypadku, gdy będzie wzbudzało wątpliwość, czy Wykonawca ujął w oferowanej cenie wszystkie wymagane przez Zamawiającego elementy przedmiotu zamówienia).
5. Zamawiający zastrzega sobie prawo odrzucenia oferty, w szczególności, jeżeli:
   a) została złożona po terminie składania ofert;
   b) jej treść jest niezgodna z warunkami zamówienia wskazanymi w zapytaniu ofertowym;
   c) została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
   d) w przypadku, gdy Wykonawca nie odpowie na wezwanie Zamawiającego lub nie przedstawi wystarczających wyjaśnień pozwalających uznać zaproponowaną cenę za rzetelną,
   e) oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia lub wykonawca nie odpowiedział na wezwanie zamawiającego, lub nie przedstawił wystarczających wyjaśnień i /lub dowodów;
   f) wykonawca nie wyraził zgody na przedłużenie terminu związania ofertą;
   g) wykonawca nie wyraził zgody na wybór jego oferty po upływie terminu związania ofertą;
   h) obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe;
   i) jeżeli wykonawca będzie podlegał wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U.2022 poz. 835 ze zm).

IX. NIEOBOWIĄZKOWE NEGOCJACJE

1. Zamawiający może prowadzić negocjacje z Wykonawcami w celu ulepszenia treści złożonych ofert.
2. Negocjacje mogą być prowadzone w szczególności w zakresie ceny, ulepszenia przedmiotu zamówienia, ulepszenia warunków realizacji, ulepszenia warunków umowy.
3. Negocjacje mogą być prowadzone w formie ustnej, za pomocą platformy do rozmów i wideokonferencji, w formie e- mail etc.
4. Po zakończeniu negocjacji zamawiający może zaprosić wykonawców do złożenia ofert dodatkowych.

X. ZAKOŃCZENIE POSTĘPOWANIA.

1. Postępowanie o udzielenie zamówienia kończy się:

1.1. Zawarciem umowy w sprawie zamówienia publicznego (w formie pisemnej, elektronicznej lub ustnej)

1.2. Unieważnieniem postępowania. Zamawiający może unieważnić postępowanie jeżeli:

a) nie otrzymał żadnej oferty
b) wszystkie oferty zostały odrzucone
c) cena oferty przekracza kwoty jakie zamawiający planował przeznaczyć na sfinansowanie zamówienia
d) oferta zawiera rażąco niską cenę.

2. **Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podawania przyczyn na każdym etapie.**

XI. PROJEKTOWANE POSTANOWIENIA UMOWY.

Projektowane postanowienia umowy zawiera załącznik nr 3

W załączeniu:

Załącznik nr 1 - Formularz ofertowy

Załącznik nr 2 – oświadczenie wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia uwzględniające przesłanki wykluczenia z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego

Załącznik nr 3 - wzór umowy

Sporządziła: Magdalena Skwara

ZASTĘPCA KIEROWNIKA
ds. Zamówień Publicznych
w Dziale Informatyki
mgr Magdalena Skwara

	Zamawiający: ***Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii*** ***im. M. Kopernika w Łodzi*** ***Ul. Pabianicka 62*** ***93-513 Łódź***
Dane wykonawcy:	
Nazwa wykonawcy: ..... Adres wykonawcy :..... Telefon osoby do kontaktu: ..... Adres e-mail osoby do kontaktu:	Adres internetowy: www..... NIP: ..... REGON: ..... Nr KRS/CEiDG: .....
FORMULARZ OFERTOWY	

W odpowiedzi na zapytanie ofertowe na **świadczenie usługi wsparcia technicznego w zakresie utrzymania i rozwoju Systemu Portal Pacjenta w Wojewódzkim Wielospecjalistycznym Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi** oferujemy wykonanie zamówienia na następujących warunkach:

1. Cena oferty:

Przedmiot zamówienia	Ilość	j.m.	Cena netto jednostkowa (j.m.)	Wartość netto	VAT %	Wartość brutto
1.	*2.*	*3.*	*4.*	*5. (2.x4.)*	*6.*	*7. (5.+6.)*
Zakup i wdrożenie funkcjonalności 2FA – w terminie 1 miesiąca od dnia podpisania umowy	**1**	**Szt.**				
Świadczenie usług wsparcia technicznego i nadzoru autorskiego w zakresie utrzymania i rozwoju Systemu Portal Pacjenta: *a) Portal Pacjenta - wydanie ISO* *b) Portal Pacjenta - przygotowanie i wnioskowanie o ISO* *c) Portal Pacjenta - podgląd listy badań z EDM* *d) Portal Pacjenta - podgląd obrazów DICOM* *e) Portal Pacjenta - integracja HL7* *f) Wsparcie funkcjonalności 2FA*	**24**	**mies.**				
Prace programistyczne 10 RBH/mies	**240**	**rbh**				
			SUMA			

2. Oferujemy termin realizacji zamówienia **24 miesięcy** od dnia udzielenia zamówienia (podpisania umowy).
3. Oferujemy termin płatności **60 dni** od dnia przesłania faktury do Zamawiającego.
4. Oświadczamy, że w cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
5. Termin związania ofertą **45 dni** od dnia przesłania na adres e-mail.
6. Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności tzw. split payment (dotyczy wykonawcy z terytorium Rzeczpospolitej Polskiej)

7. Przedstawicielem Wykonawcy wyznaczonym do nadzoru nad realizacją umowy jest: ..... ***(podać),*** nr telefonu: ..... ***(podać)*** adres e-mail: .....@..... ***(podać)***
8. Zgłoszenia kierowane będą na adres e-mail: ..... ***(podać)*** lub poprzez system zgłoszeniowy Wykonawcy. Dla incydentów krytycznych (P1) Zamawiający jest uprawniony do zgłoszenia incydentu również poza godzinami 9:00–17:00 na numer dyżurny (on-call) Wykonawcy: ..... ***(podać)*** .
9. Wykonawca oświadcza, iż **posiada / nie posiada** *skreślić niewłaściwe statusu dużego przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j.: Dz. U. z 2023 r. poz. 1709 ze zm.).
10. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
11. Zapoznałem zapoznaliśmy się i w pełni oraz bez żadnych zastrzeżeń akceptujemy treść zapytania ofertowego, wraz z wyjaśnieniami i zmianami i nie wnosimy do niego zastrzeżeń oraz przyjmuję /-jemy warunki w niej zawarte;
12. W przypadku uznania mojej(naszej) oferty za najkorzystniejszą zobowiązuję(emy) się zawrzeć umowę sporządzoną na podstawie wzoru stanowiącego załącznik do SWZ, z uwzględnieniem zmian wprowadzonych w trakcie trwania postępowania.

.....
data

.....
podpis / kwalifikowany podpis/ elektroniczny/podpis zaufany/ podpis osobisty

Załącznik nr 2

Nr sprawy: EI.273.10.III.2026

Oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia[1]

składane na podstawie art. 7 ust. 9 i uwzględniające przesłanki wykluczenia z art. 7 ust. 1

ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. 2022 poz. 835 ze zm)

Na potrzeby postępowania o udzielenie zamówienia publicznego o wartości nie przekraczającej **170 000,00 zł**

na świadczenie usługi wsparcia technicznego w zakresie utrzymania i rozwoju Systemu Portal Pacjenta w Wojewódzkim Wielospecjalistycznym Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi

oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:

Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (Dz. U. 2022 poz. 835 ze zm.)[2]

.....
data

.....
podpis / kwalifikowany podpis/ elektroniczny/podpis zaufany/ podpis osobisty

[1] Niepotrzebne skreślić

[2] Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, zwanej dalej „ustawą", z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:
1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;
3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

UMOWA nr EI.273.10.III.2026
z dnia .....

zawarta przez:
Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi wpisany do Krajowego Rejestru Sądowego Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym dla Łodzi – Śródmieścia w Łodzi, XX Wydział KRS pod numerem KRS 0000004955, REGON 000295403, NIP 729 - 23 - 45 – 599, z siedzibą w Łodzi, ul. Pabianicka 62, 93-513 Łódź
reprezentowany przez
.....
zwany dalej **Zamawiającym**
z
firmą .....
(REGON: ..... NIP: .....)
z siedzibą w ....., ulica ....., ...-..... .....
wpisaną do Krajowego Rejestru Sądowego pod numerem .....
reprezentowaną przez: .....
zwaną dalej **Wykonawcą**

W rezultacie przeprowadzenia postępowania o udzielenie zamówienia publicznego zgodnie z art. 2 ust. 1 pkt. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (tj. Dz. U. z 2024 r., poz. 1320 ze zm.), została zawarta umowa,o poniższej treści.

§1 PRZEDMIOT UMOWY

1. Przedmiotem niniejszej umowy jest jednorazowy zakup i wdrożenie funkcjonalności **2FA (uwierzytelnianie dwuskładnikowe)** oraz świadczenie przez Wykonawcę na rzecz Zamawiającego usług wsparcia technicznego i nadzoru autorskiego w zakresie utrzymania i rozwoju **Systemu Portal Pacjenta** (zwanego dalej „Systemem"). Odbiór 2FA nastąpi na podstawie protokołu odbioru podpisanego przez Zamawiającego po pozytywnym przejściu testów akceptacyjnych. Wynagrodzenie, o którym mowa w § 5A ust. 2 lit. a, jest należne po dokonaniu odbioru 2FA. Wdrożenie funkcjonalności 2FA oznacza uruchomienie mechanizmu uwierzytelniania dwuskładnikowego w środowisku produkcyjnym Systemu, wraz z konfiguracją, dokumentacją użytkownika/administratora oraz wykonaniem testów akceptacyjnych zgodnie z Załącznikiem nr 7 (Testy akceptacyjne 2FA).
2. Zakres wsparcia obejmuje następujące funkcjonalności systemu:
   a) Portal Pacjenta - wydanie ISO
   b) Portal Pacjenta - przygotowanie i wnioskowanie o ISO
   c) Portal Pacjenta - podgląd listy badań z EDM
   d) Portal Pacjenta - podgląd obrazów DICOM
   e) Portal Pacjenta - integracja HL7
   f) Wsparcie funkcjonalności 2FA
   g) Prace programistyczne do 10 roboczogodzin w miesiącu, obejmujące w szczególności: rozwój, wprowadzanie dodatkowych funkcjonalności i ich modyfikacje.
3. Wykonawca zapewnia wsparcie obejmujące w szczególności:
   a) analizę i diagnozę błędów zgłaszanych przez Zamawiającego,
   b) konsultacje techniczne dotyczące działania i konfiguracji Systemu,
   c) opracowanie poprawek i aktualizacji niezbędnych do prawidłowego działania Systemu,
   d) wprowadzanie aktualizacji bezpieczeństwa oraz obsługę wykrytych podatności,
   e) wdrażanie uzgodnionych zmian funkcjonalno-technicznych wynikających z analizy ryzyka dla Systemu w zakresie bezpieczeństwa informacji i ochrony danych, realizowane na podstawie przekazanych Wykonawcy rekomendacji oraz w ramach wsparcia i prac programistycznych,
   f) współpracę z Działem Informatyki Zamawiającego w zakresie przyjmowania, rejestracji i obsługi zgłoszeń dotyczących Systemu z wyłączeniem utrzymania infrastruktury Zamawiającego, o ile Strony nie postanowią inaczej.

§ 2 ZAKRES I SPOSÓB ŚWIADCZENIA USŁUG

1. Wsparcie świadczone będzie zdalnie, w dni robocze (poniedziałek–piątek),w godzinach 9:00–17:00.
2. Zgłoszenia kierowane będą na adres e-mail: ..... lub poprzez system zgłoszeniowy Wykonawcy. Dla incydentów krytycznych (P1) Zamawiający jest uprawniony do zgłoszenia incydentu również poza godzinami 9:00–17:00 na numer dyżurny (on-call) Wykonawcy: ..... . Wykonawca potwierdza przyjęcie zgłoszenia P1 niezwłocznie, nie później niż w czasie reakcji określonym w ***Załączniku nr 2***.
3. Wykonawca zapewni:
   a) czasy reakcji – zgodnie z **załącznikiem nr 2**,
   b) czas usunięcia błędu krytycznego – zgodnie z **załącznikiem nr 2**.
4. Klasyfikacja incydentów wraz z czasem reakcji została opisana w **załączniku nr 2**.

§ 3 CZAS TRWANIA UMOWY

Umowa zostaje zawarta na czas określony **24 miesiące** od dnia podpisania umowy.

§ 4 NADZÓR NAD REALIZACJĄ UMOWY

1. Pracownikiem upoważnionym do reprezentowania Zamawiającego jest: ..... - pracownik zamawiającego – Dział Informatyki (tel.: 042 689 ....., e-mail:.....@kopernik.lodz.pl).
2. Osobą odpowiedzialną za realizację umowy ze strony Zamawiającego jest Kierownik Działu Informatyki - ..... lub osoba przez niego upoważniona. Tel. 42 689-58-68, e-mail .....@kopernik.lodz.pl
3. Przedstawicielem Wykonawcy wyznaczonym do nadzoru nad realizacją umowy jest: ....., nr telefonu: ..... adres e-mail: .....@.....
4. O każdej zmianie powyższej wymienionej osoby lub jego danych kontaktowych Strona jest zobowiązana niezwłocznie poinformować drugą Stronę w formie pisemnej.

§ 5 A WARTOŚĆ UMOWY I ZASADY PŁATNOŚCI

1. Wynagrodzenie Wykonawcy z tytułu realizacji niniejszej Umowy wynosi: netto ..... zł (słownie: ..... złote .../100) brutto: ..... zł (słownie: ..... zł 00/100).
2. Na wynagrodzenie Wykonawcy wskazane w ust. 1 składa się:
   a) Wynagrodzenie za zakup i wdrożenie **2FA** w kwocie: netto ..... zł brutto: ..... zł (słownie: ..... zł 00/100), płatne jednorazowo wraz z pierwszą fakturą;
   b) miesięczne wynagrodzenie w wysokości z tytułu usług wsparcia i nadzoru autorskiego netto: ..... zł, brutto: ..... zł (słownie: ..... złotych ...../100) płatne z dołu po zakończeniu każdego miesiąca kalendarzowego, na podstawie prawidłowo wystawionej i doręczonej faktury.
   c) Miesięczne wynagrodzenie za wykorzystane roboczogodziny, o których mowa w §1ust. 2 lit.g. Wynagrodzenie za 1 rbh wynosi ..... zł netto plus należny podatek VAT.
3. Zapłata będzie realizowana przelewem na konto bankowe Wykonawcy w terminie **60 dni** od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury. Do faktury obowiązkowo muszą być załączone dokumenty (załączniki) wymagane umową. Dokumentami (załącznikami) wymaganymi umową są w szczególności:
   a. dla faktury obejmującej 2FA – protokół odbioru 2FA, o którym mowa w §1 ust. 1;
   b. dla faktur miesięcznych – miesięczny raport SLA (rejestr zgłoszeń, czasy reakcji i rozwiązania, statusy) oraz zestawienie wykorzystania roboczogodzin prac programistycznych zaakceptowane przez osobę wskazaną w §4 ust. 2.
4. Zamawiający oświadcza, że będzie realizować płatności za faktury z zastosowaniem mechanizmu podzielonej płatności tzw. split payment. Podzieloną płatność tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata odszkodowania), a także za świadczenia zwolnione z VAT lub opodatkowane stawką 0%.
5. Zapłata nastąpi przelewem na rachunek bankowy Wykonawcy wskazany w przesłanej przez niego fakturze pod warunkiem jego zgodności z danymi ujawnionymi w Białej Księdze podatków VAT. Data dostarczenia danej faktury do Zamawiającego nie może być wcześniejsza niż data wykonania zamówienia, którego ta faktura dotyczy.
6. Wykonawca oświadcza, że jest podatnikiem podatku od towarów i usług (VAT).

7. Dniem zapłaty wynagrodzenia jest dzień obciążenia rachunku bankowego Zamawiającego.

§ 5 B SPOSÓB PRZEKAZANIA FAKTURY WRAZ Z ZAŁĄCZNIKAMI

1. Z dniem wejścia w życie wobec Wykonawcy obowiązku korzystania z Krajowego Systemu e-Faktur (KSeF), Wykonawca zobowiązany jest do wystawiania faktur ustrukturyzowanych, zgodnie z aktualnym schematem logicznym (e-Faktura). Za datę dostarczenia faktury, w tym przypadku przyjmuje się dzień przydzielenia fakturze numeru identyfikującego w systemie KSeF.
   (a) Faktura ustrukturyzowana (KSeF), oprócz elementów wymaganych ustawą z dnia 11 marca 2004r. o podatku od towarów i usług (t.j. Dz. U. z 2025 r. poz. 775 z późn. zm.), powinna zawierać w polu dedykowanym (np. „Numer Zamówienia" lub „Opis") numer Umowy oraz numer zamówienia (jeśli dotyczy), pod rygorem uznania faktury za nieprawidłowo wystawioną.
   (b) Z uwagi na brak możliwości przesyłania załączników wymaganych umową przez system KSeF, Wykonawca zobowiązany jest przekazać załączniki wymagane umową drogą elektroniczną, nie później niż w terminie **3 dni** roboczych od dnia wystawienia faktury w systemie KSeF, na adres poczty elektronicznej Zamawiającego: **AE:PL-46045-75938-SSJRH-26**.
   (c) Brak skutecznego wystawienia faktury ustrukturyzowanej w systemie KSeF, wystawienie faktury wadliwej (merytorycznie lub formalnie) lub brak dostarczenia wymaganych umową załączników powoduje, że termin zapłaty, wskazany w umowie, nie biegnie do czasu otrzymania przez Zamawiającego faktury ustrukturyzowanej w systemie KSeF, faktury korygującej ustrukturyzowanej (tj. nadania jej numeru identyfikującego KSeF) lub załączników wymaganych umową.
   (d) W przypadku awarii systemu KSeF (po stronie Ministerstwa Finansów lub Wykonawcy), Wykonawca zobowiązany jest do wystawienia faktury w trybie offline (wizualizacja faktury z kodem QR) i dostarczenia jej na adres poczty elektronicznej Zamawiającego: **AE:PL-46045-75938-SSJRH-26**. Wykonawca zobowiązany jest do wprowadzenia takiej faktury do systemu KSeF niezwłocznie po ustąpieniu awarii.
2. Do dnia wejścia w życie, wobec Wykonawcy, obowiązku korzystania z Krajowego Systemu e-Faktur (KSeF), Wykonawca ma możliwość wystawiania faktury w formie papierowej lub elektronicznej i dostarczania jej osobiście, za pośrednictwem usług pocztowych lub kurierskich, pocztą elektroniczną skrzynki oraz za pomocą platformy elektronicznego fakturowania (PEF).
   Za datę dostarczenia faktury, w tym przypadku, przyjmuje się:
   1) dzień dostarczenia wraz z załączonymi dokumentami;
   2) dzień wpływu do kancelarii Zamawiającego;
   3) dzień wpływu na skrzynkę poczty elektronicznej Zamawiającego: **AE:PL-46045-75938-SSJRH-26**;
   4) dzień doręczenia za pomocą platformy elektronicznego fakturowania (PEF) dostępnej pod adresem: https://www.brokerinfinite.efaktura.gov.pl/
      Numer PEPPOL: 7292345599 (numer PEPPOL to NIP Centrum).
      (a) Wykonawca zobowiązany jest umieścić na każdej fakturze, w widocznym miejscu numer Umowy oraz numer zamówienia (jeśli dotyczy), pod rygorem uznania faktury za nieprawidłowo wystawioną.
      (b) Zgodnie z zapisami w umowie w przypadku braku dostarczenia faktury, dostarczenie nieprawidłowej faktury lub niedostarczenie załączników wymaganych umową powoduje, że termin zapłaty nie biegnie do czasu skutecznego dostarczenia faktury (ewentualnie duplikatu), dostarczenia prawidłowo wystawionej faktury (korekta) lub dostarczenia załączników wymaganych umową.

§ 6 OBOWIĄZKI STRON

1. Wykonawca zobowiązuje się do należytego świadczenia usług zgodnie z zasadami wiedzy technicznej oraz postanowieniami umowy.
2. Wykonawca oświadcza, że dysponuje niezbędną wiedzą, doświadczeniem i profesjonalnymi kwalifikacjami, a także potencjałem ekonomicznym i technicznym oraz osobami zdolnymi do wykonania Umowy.
3. Wykonawca jest zobowiązany wykonać Przedmiot Umowy z należytą starannością, z zasadami sztuki i wiedzą zawodową wymaganą od profesjonalisty, a także obowiązującymi normami i przepisami prawa.
4. Wykonawca zobowiązuje się na bieżąco współdziałać z Zamawiającym w celu sprawnej i należytej realizacji Umowy.
5. Wykonawca jest zobowiązany do bezzwłocznego informowania Zamawiającego o wszelkich zagrożeniach dla realizacji Przedmiotu Umowy, w szczególności dotyczących zarówno terminów jak i zakresu rzeczowego Umowy.
6. Zamawiający zobowiązuje się do:

a) przekazywania Wykonawcy kompletnych informacji dotyczących zgłaszanych błędów,
b) zapewnienia kontaktu z osobami upoważnionymi do współpracy z Wykonawcą,
c) zapewnienia dostępu do środowiska testowego (jeśli wymagane).

7. Prace programistyczne, o których mowa w §1 (10 roboczogodzin w miesiącu), realizowane są wyłącznie na podstawie zleceń Zamawiającego w formie zgłoszenia (e-mail/system zgłoszeniowy), zawierającego opis zadania oraz priorytet.
8. Wykonawca, przed rozpoczęciem prac, przedstawia szacunkową pracochłonność (w roboczogodzinach) i harmonogram realizacji; rozpoczęcie prac wymaga akceptacji Zamawiającego w formie dokumentowej.
9. Niewykorzystane w danym miesiącu roboczogodziny co do zasady nie przechodzą na kolejne miesiące. Wyjątek stanowią roboczogodziny niewykorzystane z przyczyn organizacyjnych, których przeniesienie zostało uzgodnione i zaplanowane przez Strony z co najmniej miesięcznym wyprzedzeniem, w formie pisemnej (w szczególności e-mail), ze wskazaniem liczby godzin oraz miesiąca, na który zostają przeniesione. W pozostałym zakresie Wykonawca nie jest uprawniony do żądania dodatkowego wynagrodzenia za prace przekraczające miesięczny limit bez uprzedniej, pisemnej zgody Zamawiającego.
10. Rozliczenie roboczogodzin następuje na podstawie zestawienie wykorzystania roboczogodzin prac programistycznych, o którym mowa w §5A ust. 3, zatwierdzonego przez Zamawiającego.

§ 7 ODPOWIEDZIALNOŚĆ

1. Wykonawca ponosi odpowiedzialność za szkody wynikłe z nienależytego wykonania umowy, z wyłączeniem utraconych korzyści Zamawiającego, z zastrzeżeniem §7 ust. 4.
2. Wykonawca oświadcza, że za działania lub zaniechania osób trzecich (kooperantów Wykonawcy), z którym Wykonawca współpracuje w celu realizacji niniejszej umowy odpowiada jak za własne działania lub zaniechania.
3. Odpowiedzialność Wykonawcy ograniczona jest do wysokości wynagrodzenia wypłaconego mu na podstawie niniejszej umowy w okresie ostatnich 24 miesięcy.
4. Ograniczenie odpowiedzialności, o którym mowa w ust. 3, nie ma zastosowania do szkód i roszczeń wynikających z:
   a. naruszenia poufności (§10) lub ochrony danych osobowych (§11 oraz Umowa powierzenia),
   b. umyślności lub rażącego niedbalstwa Wykonawcy lub osób, za które ponosi odpowiedzialność,
   c. roszczeń osób trzecich oraz kar/administracyjnych kar pieniężnych pozostających w związku z działaniem lub zaniechaniem Wykonawcy.
5. Wykonawca nie ponosi odpowiedzialności z tytułu niewykonania lub nienależytego wykonania umowy wskutek:
   a. niedostarczenia przez Zamawiającego, dostarczenia nieprawdziwych lub dostarczenia niekompletnych informacji niezbędnych do realizacji umowy;
   b. błędnego działania lub niedziałania infrastruktury teleinformatycznej Zamawiającego z przyczyn niezwiązanych z działaniem Portalu.
6. Żadna ze Stron nie będzie ponosić odpowiedzialności za opóźnienie lub niewykonanie zobowiązań wynikających z umowy spowodowane siłą wyższą. Jeśli którakolwiek ze Stron nie może spełnić swoich zobowiązań z powodu zaistnienia siły wyższej, zawiadomi drugą Stronę w formie pisemnej o tego rodzaju okolicznościach, a druga Strona dokona uzasadnionej zmiany terminu realizacji zobowiązania. Jeżeli po upływie 3 miesięcy okoliczności siły wyższej nie ustaną, Strony będą mogły uzgodnić dalszy sposób postępowania lub rozwiązać umowę. Pod pojęciem siły wyższej rozumie się zjawiska o charakterze żywiołowym tj. powódź, pożar, huragan, trzęsienie ziemi oraz zjawiska o charakterze społecznym tj. strajki, zamieszki czy działania zbrojne, które w sposób obiektywny i niezależny od woli stron czynią niemożliwym wykonywanie niniejszej umowy.
7. Wykonawca udziela Zamawiającemu niewyłącznej, nieograniczonej terytorialnie licencji na czas nieoznaczony do korzystania z Systemu oraz wszelkich modyfikacji, poprawek i utworów zależnych powstałych w związku z realizacją niniejszej umowy, w zakresie niezbędnym do utrzymania i eksploatacji Systemu przez Zamawiającego, w tym do instalacji, uruchamiania, wykonywania kopii zapasowych, modyfikowania i zlecania utrzymania osobom trzecim.
8. W ramach wynagrodzenia Wykonawca przekaże Zamawiającemu dokumentację administracyjną i wdrożeniową dotyczącą 2FA oraz zmian wykonanych w ramach prac programistycznych, nie później niż w terminie 14 dni od ich wdrożenia.
9. Wykonawca oświadcza, że udzielenie licencji, o której mowa w ust. 1, nie narusza praw osób trzecich; w razie zgłoszenia roszczeń osób trzecich Wykonawca zwolni Zamawiającego z odpowiedzialności i pokryje uzasadnione koszty obrony oraz zasądzone świadczenia.

§ 8 KARY UMOWNE

1. Strony ustalają odpowiedzialność za niewykonanie lub nienależyte wykonanie niniejszej umowy w formie kar umownych.

2. Strony ustalają, że Zamawiający naliczy Wykonawcy następujące kary umowne:
   1) w przypadku zwłoki w terminie usunięcia **incydentu krytycznego** w wysokości **0,5%** miesięcznego wynagrodzenia brutto, za każdy dzień zwłoki;
   2) w przypadku zwłoki w terminie usunięcia **incydentu wysokiego** w wysokości **0,2%** miesięcznego wynagrodzenia brutto, za każdy dzień zwłoki;
   3) w przypadku zwłoki w terminie usunięcia **incydentu standardowego** w wysokości **0,1%** miesięcznego wynagrodzenia brutto, za każdy dzień zwłoki;
   4) w przypadku ujawnienia informacji poufnych, o których mowa w § 10 umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5000,00 zł (słownie: jeden tysiąc złotych 00/100) za każdy przypadek ujawnienia informacji;
   5) w przypadku naruszenia ochrony powierzonych do przetwarzania danych osobowych, o których mowa w § 11, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5000,00 zł (słownie: jeden tysiąc złotych 00/100) za każdy przypadek naruszenia postanowień;
   6) w przypadku niewykonania lub nienależytego wykonania obowiązku niezwłocznego zgłoszenia naruszenia danych osobowych lub incydentu bezpieczeństwa (w szczególności w terminie określonym w Umowie powierzenia), Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5000,00 zł (słownie: jeden tysiąc złotych 00/100)za każdy przypadek;
   7) W razie odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy albo w razie odstąpienia od umowy przez Wykonawcę z przyczyn nieleżących po stronie Zamawiającego, Wykonawca zapłaci karę umowną w wysokości **2%** wynagrodzenia brutto określonego w § 5 ust. 1 umowy.
3. Maksymalna wartość kar umownych, naliczonych w przypadkach wskazanych w niniejszej umowie, nie przekroczy 30% wartości wynagrodzenia brutto opisanego w §5 ust. 1, z wyłączeniem kar za naruszenie poufności (§10) oraz ochrony danych osobowych (§11), które nie podlegają limitowi.
4. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przekraczającego wysokość zastrzeżonych kar umownych zgodnie z zasadami określonymi w przepisach powszechnie obowiązującego prawa.

§ 9 ZMIANA I ROZWIĄZANIE UMOWY

1. Zamawiający przewiduje możliwość zmiany postanowień zawartej Umowy w szczególności w przypadkach:
   1) Zmiana terminu realizacji / harmonogramu – w przypadku:
      a) wystąpienia siły wyższej lub innych okoliczności niezależnych od Stron, uniemożliwiających realizację Umowy w terminie;
      b) opóźnień wynikających z przyczyn leżących po stronie Zamawiającego, w szczególności nieterminowego przekazania danych, materiałów, dostępów, akceptacji lub środowisk;
      c) konieczności wykonania dodatkowych testów, migracji lub prac bezpieczeństwa wynikających z decyzji Zamawiającego, audytu lub zaleceń bezpieczeństwa.
   2) Zmiana sposobu realizacji usług / procedur / kanałów zgłoszeń – w szczególności w razie:
      a) zmiany infrastruktury lub architektury środowiska Zamawiającego (w tym hostingu, domen, certyfikatów, mechanizmów uwierzytelniania, narzędzi monitoringu);
      b) wdrożenia nowych narzędzi obsługi zgłoszeń lub zmian organizacyjnych po stronie Zamawiającego;
      c) konieczności dostosowania do wymogów bezpieczeństwa lub ciągłości działania.
   3) Zmiana zakresu usług (rozszerzenie lub ograniczenie) – w przypadku:
      a) konieczności dostosowania Systemu do zmian przepisów prawa, wytycznych organów nadzorczych lub standardów bezpieczeństwa;
      b) ujawnienia błędów, podatności lub ryzyk bezpieczeństwa wymagających modyfikacji wykraczających poza standardowe utrzymanie;
      c) konieczności integracji Systemu z systemami Zamawiającego lub usługami zewnętrznymi (API), w zakresie uzgodnionym przez Strony.
   4) Zmiana wynagrodzenia – wyłącznie w przypadku:
      a) waloryzacji na zasadach określonych w § 9 ust.3 Umowy;
      b) zmiany zakresu usług (rozszerzenie lub ograniczenie) – przy czym zmiana wynagrodzenia następuje proporcjonalnie do uzasadnionego wpływu zmiany na koszty realizacji i wymaga uprzedniej wyceny oraz akceptacji Zamawiającego;
      c) zmiany stawki podatku od towarów i usług (VAT) – w takim przypadku zmianie ulega wyłącznie wynagrodzenie brutto, przy niezmienionym wynagrodzeniu netto.
   5) Zmiana parametrów SLA – w przypadku:
      a) zmiany krytyczności Systemu lub sposobu jego wykorzystania;
      b) zmiany godzin pracy Zamawiającego lub konieczności zapewnienia dyżuru poza godzinami pracy;

c) wdrożenia dodatkowych mechanizmów monitoringu i automatyzacji wpływających na czasy reakcji/usunięcia.

6) **Zmiany w zakresie ochrony danych osobowych i bezpieczeństwa informacji** – w przypadku:
   a) konieczności dostosowania środków technicznych i organizacyjnych do RODO lub innych powszechnie obowiązujących przepisów, zaleceń CSIRT, audytu lub testów bezpieczeństwa;
   b) konieczności aktualizacji procedur obsługi incydentów i naruszeń (w tym kanałów, terminów, eskalacji i raportowania).

2. Zmiany, o których mowa w ust. 1 pkt 3–5, wymagają sporządzenia opisu zmiany obejmującego co najmniej: zakres, uzasadnienie, wpływ na termin, wpływ na SLA, koszt (jeżeli dotyczy) oraz plan wdrożenia i testów. Rozpoczęcie realizacji zmiany wymaga uprzedniej akceptacji Zamawiającego w formie pisemnej, a w przypadku zmian niewpływających na wynagrodzenie – co najmniej w formie dokumentowej (e-mail).
3. Możliwość zmiany wynagrodzenia Wykonawcy przy zastosowaniu średniorocznego wskaźnika cen towarów i usług konsumpcyjnych ogłaszanego w komunikacie Prezesa Głównego Urzędu Statystycznego („CPI GUS").
   a) Waloryzacja może skutkować zarówno **podwyższeniem, jak i obniżeniem** wynagrodzenia, odpowiednio do zmiany CPI GUS.
   b) Pierwsza waloryzacja może nastąpić **po upływie 12 miesięcy** od dnia zawarcia Umowy, a każda kolejna **nie częściej niż raz na 12 miesięcy**.
   c) Waloryzacja jest dokonywana na podstawie wniosku Strony (Zamawiającego albo Wykonawcy) z uzasadnieniem oraz wskazaniem wartości CPI GUS, przy czym waloryzacja przysługuje wyłącznie w zakresie świadczeń wykonywanych po dacie wejścia w życie zmiany wynagrodzenia.
   d) Wysokość zmiany wynagrodzenia oblicza się według wzoru: **Wn = W0 × (CPI/100)**, gdzie: **Wn** – nowe wynagrodzenie miesięczne brutto, **W0** – dotychczasowe wynagrodzenie miesięczne brutto, **CPI** – CPI GUS (średnioroczny) ogłoszony za rok poprzedzający złożenie wniosku (lub inny rok referencyjny wskazany w ust. 4).
   e) Zmiana wynagrodzenia wymaga **aneksu w formie pisemnej** i obowiązuje od **pierwszego dnia miesiąca następującego po miesiącu**, w którym podpisano aneks.
   f) W przypadku zaprzestania ogłaszania CPI GUS, zastosowanie ma wskaźnik publikowany przez GUS najbardziej zbliżony charakterem do CPI (w szczególności wskaźnik inflacji dla gospodarstw domowych), a gdyby i on nie był publikowany – inny oficjalny wskaźnik publikowany przez GUS odnoszący się do zmian cen konsumpcyjnych; w razie braku publikacji takich wskaźników – wskaźnik HICP publikowany przez Eurostat dla Polski.
   g) Maksymalna łączna wartość zmiany wynagrodzenia w okresie obowiązywania Umowy nie może przekroczyć **±50%** w stosunku do wartości wynagrodzenia brutto określonego w § 5 ust. 1.
   h) Zamawiający może odmówić dokonania waloryzacji do czasu usunięcia przez Wykonawcę stwierdzonych naruszeń Umowy, w szczególności naruszeń wymagań SLA lub zaległości w realizacji obowiązków umownych.
4. Wszystkie zmiany dotyczące ustaleń zawartych w niniejszej umowie, za wyjątkiem określonych w ust. 1 pkt. 4 lit. c , powyżej wymagają każdorazowo formy pisemnej pod rygorem nieważności. Aneksy będą ważne po ich podpisaniu przez obie Strony.
5. Zmiana umowy określona w ust. 1 pkt. 4 lit. c powyżej, obowiązuje z datą jej wprowadzenia w życie na podstawie odrębnych przepisów.
6. Zamawiającemu przysługuje **prawo rozwiązania niniejszej umowy** z zachowaniem jednomiesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego. Oświadczenie o wypowiedzeniu winno być sporządzone w formie pisemnej pod rygorem nieważności w przypadku naruszenia postanowień umownych w szczególności:
   1) wadliwego lub sprzecznego z umową wykonania umowy,
   2) gdy suma naliczonych kar umownych Wykonawcy przekroczy 30% całkowitego wynagrodzenia brutto określonego w § 5 ust. 1 umowy
7. W przypadku, o którym mowa w ust. 6, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania zrealizowanej części umowy.

§ 10 AUDYT I POUFNOŚĆ DANYCH

1. Wszelkie informacje uzyskane przez Strony w związku z wykonywaniem umowy stanowią informacje poufne i stanowią tajemnicę przedsiębiorstwa Stron. Strony zobowiązują się do nieujawniania tych informacji osobom trzecim bez uprzedniej zgody drugiej Strony wyrażonej na piśmie.
2. Obowiązek zachowania poufności obowiązuje również po rozwiązaniu lub wygaśnięciu umowy.
3. Wykonawca zobowiązuje się do zachowania w poufności wszystkich informacji w szczególności dotyczących Zamawiającego personelu, współpracowników i podmiotów współpracujących z Zamawiającym, jakie Wykonawca uzyska w toku realizacji Umowy.

4. Wszelkie informacje o Zamawiającym uzyskane przez Wykonawcę w związku z realizacją Przedmiotu Umowy mogą być wykorzystane tylko w celu wykonania umowy.
5. Obowiązek określony w ust. 1 nie dotyczy:
   5.1. informacji publicznie dostępnych,
   5.2. informacji, które były znane Stronie przed otrzymaniem od drugiej Strony i nie były objęte zobowiązaniem do poufności względem jakiegokolwiek podmiotu,
   5.3. obowiązku ujawnienia wynikającego z przepisów powszechnie obowiązujących.
6. Zobowiązanie do zachowania poufności nie stoi na przeszkodzie ujawnieniu informacji na uprawnione żądanie sądu lub organu administracji oraz w postępowaniu sądowym lub administracyjnym, jeżeli jest to potrzebne dla jego rozstrzygnięcia i przy zachowaniu możliwych środków ochrony ujawnianych informacji przed ich publicznym rozpowszechnieniem – po uprzednim pisemnym poinformowaniu drugiej Strony o żądaniu ujawnienia.
7. Wykonawca odpowiada za podjęcie i zapewnienie wszelkich niezbędnych środków zapewniających dochowanie zasady poufności, określonej w ust. 1 - 4, przez swoich pracowników i Podwykonawców.

§ 11 OCHRONA DANYCH OSOBOWYCH I POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Zamawiający powierza Wykonawcy przetwarzanie danych osobowych w imieniu Zamawiającego, na zasadach określonych w *Umowie powierzenia przetwarzania danych osobowych*, stanowiącej **załącznik nr 3, Załącznik nr 4 Bezpieczeństwo informacji oraz Załącznik nr 5 Oświadczenie o zachowaniu poufności** do niniejszej umowy oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w Rozporządzeniu 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.
2. Wykonawca odpowiada za podjęcie i zapewnienie wszelkich niezbędnych środków zapewniających dochowanie zasad ochrony danych przetwarzanych w ramach zawartej Umowy przez swoich pracowników oraz przez Podwykonawców.
3. Wykonawca zobowiązuje się do przestrzegania zasad określonych w **Załączniku nr 4** do umowy - **„Bezpieczeństwo Informacji".**
4. Zamawiający dopuszcza usługę zdalnego serwisu realizowanej za pośrednictwem sieci publicznej Internet na zasadach określonych w Załączniku nr 4 do umowy - **„Bezpieczeństwo Informacji".**
5. Przed rozpoczęciem prac objętych niniejszą Umową Wykonawca zobowiązuje się dostarczyć wykaz osób, które będą mogły mieć dostęp do informacji poufnych podczas realizacji umowy oraz dostarczy podpisane przez te osoby Oświadczenia o zachowaniu poufności stanowiące **Załącznik nr 5** do umowy „Oświadczenie o zachowaniu poufności".
6. Wykonawca oświadcza, że poinformował osoby, których dane zostały podane w treści Umowy o przekazaniu ich danych do Zamawiającego oraz przekazał im informacje, o których mowa w **Załączniku nr 6 do umowy** (Klauzula informacyjna dla osób reprezentujących Wykonawcę).
7.

§ 12 ZAKAZ CESJI WIERZYTELNOŚCI I POWIADAMIANIE O ZMIANACH

1. Wykonawca nie może w jakikolwiek sposób, pod rygorem nieważności takiej czynności, przenieść wierzytelności wynikającej z niniejszej umowy, w szczególności w drodze cesji, poręczenia lub factoringu, na osobę trzecią bez uprzedniej pisemnej zgody Zamawiającego oraz bez spełnienia warunków wynikających z przepisów powszechnie obowiązującego prawa. Każda czynność mająca na celu zmianę wierzyciela Zamawiającego może nastąpić dopiero po uprzednim wyrażeniu zgody przez podmiot tworzący, zgodnie w art. 54 ust. 5 ustawy z dnia 15 kwietnia 2011r. o działalności leczniczej.
2. Każda ze stron zobowiązana jest powiadomić niezwłocznie drugą stronę o zmianach organizacyjno – prawnych, które miały miejsce w okresie związania umową, jeśli mają wpływ na realizację umowy lub sposób wystawiania dokumentów rozliczeniowych, złożyć komplet dokumentów wskazujących następcę prawnego.

§ 13 POSTANOWIENIA KOŃCOWE

1. Zamawiający oświadcza, iż posiada status dużego przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j.: Dz. U. z 2023 r. poz. 1709 ze zm.).
2. Wykonawca oświadcza, iż (nie posiada)..... statusu dużego przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j.: Dz. U. z 2023 r. poz. 1709 ze zm.).

3. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności kodeksu cywilnego.
4. Wykonawca oświadcza że jest mu znany stan majątkowy Zamawiającego w rozumieniu dyspozycji z art. 490 § 2 ustawy k.c.
5. Strony zgodnie postanawiają, że w przypadku zaistnienia pomiędzy nimi sporu dotyczącego niniejszej umowy lub pozostającego w związku z nią, przed skierowaniem sprawy na drogę sądową, podejmą próbę rozwiązania sporu w postępowaniu mediacyjnym. W tym celu Strona, która dochodzić będzie roszczeń od drugiej strony, zobowiązana będzie przed wytoczeniem powództwa do przeprowadzenia postępowania mediacyjnego, o którym mowa w art. 183^1 k.p.c.. Brak przeprowadzenia postępowania mediacyjnego skutkować będzie podniesieniem przez drugą stronę w postępowaniu cywilnym zarzutu z art. 202^1 k.p.c.. Wszelkie spory mogące wyniknąć z/lub związane z Umową podlegają rozstrzygnięciu przez właściwy dla siedziby Zamawiającego sąd powszechny.
6. W sprawach nieuregulowanych niniejszą umową, zastosowanie mają przepisy Kodeksu Cywilnego Strony wyłączają jednak między sobą zastosowanie art. 552 KC.
7. W przypadku spraw sądowych, dotyczących rekompensat określonych w art. 10 ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych, dowodem poniesienia przez Wykonawcę kosztów odzyskiwania danej należności nie może być dowód z zeznań świadków. Strony zgodnie oświadczają, iż w przypadku opóźnienia w zapłacie jakiejkolwiek należności z tytułu wykonania niniejszej umowy, Wykonawcy przysługuje jedno roszczenie o zapłatę rekompensaty za koszty odzyskiwania należności, niezależnie od ilości wystawionych faktur w związku z wykonaniem niniejszej umowy.
8. Umowę sporządzono w **trzech jednobrzmiących** egzemplarzach - dwa dla Zamawiającego i jeden dla Wykonawcy.

Załączniki:

1) Załącznik nr 1 – formularz ofertowy
2) Załącznik nr 2 - SLA
3) Załącznik nr 3 - Umowa powierzenia danych
4) Załącznik nr 4 – Bezpieczeństwo informacji
5) Załącznik nr 5 – Oświadczenie o zachowaniu poufności
6) Załącznik nr 6 - Klauzula informacyjna dla Wykonawcy
7) Załącznik nr 7 – Testy akceptacyjne i protokół odbioru 2FA

Zamawiający **Wykonawca**

1. Zakres SLA

SLA obejmuje wsparcie techniczne, utrzymanie oraz reagowanie na incydenty dotyczące Portalu Pacjenta, w szczególności:
- dostępności Portalu Pacjenta,
- funkcjonalności krytycznych (logowanie, 2FA, podgląd obrazów DICOM-PACS, integracja HL7),
- bezpieczeństwa informacji i danych osobowych,
- integracji z systemami zewnętrznymi,
- zgodności z obowiązującymi przepisami prawa.

2. Godziny wsparcia

(a) Standardowe godziny wsparcia: dni robocze 9:00–17:00.
(b) Incydenty krytyczne obsługiwane są również poza godzinami pracy **w trybie dyżurowym.**
(c) Czas reakcji liczony jest od momentu przesłania zgłoszenia incydentu.

3. Klasyfikacja incydentów i czasy realizacji

3.1 Incydent krytyczny (P1)

Definicja:
- całkowita niedostępność Portalu Pacjenta,
- brak możliwości logowania się pacjentów - w tym 2FA (dla większości użytkowników),
- incydent bezpieczeństwa lub podejrzenie naruszenia danych (poufność/integralność/dostępność).

SLA:
- maksymalny czas reakcji: do 1 godziny,
- maksymalny czas rozwiązania: do 8 godzin.

3.2 Incydent wysoki (P2)

Definicja:
- brak dostępu do podpisanych opisów,
- brak możliwości podglądu badania,
- brak możliwości pobrania obrazu ISO badania,
- częściowa niedostępność Portalu Pacjenta,
- niedostępność wybranych funkcji systemu,
- istotne błędy wpływające na obsługę pacjentów.

SLA:
- maksymalny czas reakcji: do 10 godzin,
- maksymalny czas rozwiązania: do 3 dni roboczych.

3.3 Incydent standardowy (P3)

Definicja:
- błędy niekrytyczne,
- problemy kosmetyczne lub funkcjonalne,
- zgłoszenia informacyjne.

SLA:
- maksymalny czas reakcji: do 1 dnia roboczego,
- maksymalny czas rozwiązania: do 7 dni roboczych.

4. Bezpieczeństwo

(a) Incydenty bezpieczeństwa traktowane są jako incydenty krytyczne.
(b) Wykonawca współpracuje przy analizie i obsłudze incydentów oraz realizacji obowiązków prawnych.

5. Raportowanie i eskalacja

(a) Wykonawca prowadzi rejestr zgłoszeń.
(b) Zapewnia tryb eskalacji dla incydentów krytycznych.

Załącznik nr 3 do umowy nr EI.273.10.III.2026

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Łodzi przez:
Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi
wpisane do Krajowego Rejestru Sądowego Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej w Sądzie Rejonowym dla Łodzi – Śródmieścia w Łodzi, XX Wydział KRS pod numerem 0000004955, REGON 000295403, NIP 729 - 23 - 45 - 599)
z siedzibą w Łodzi, ul. Pabianicka 62
reprezentowany przez **Andrzeja Kasprzyka - Dyrektora**
zwane dalej **Administratorem**
z
..... przy ul. ....., wpisaną do Krajowego Rejestru Sądowego ....., ... KRS: ....., NIP: .....,REGON: .....
reprezentowanym przez: ..... – ..... zwany dalej **Podmiotem Przetwarzającym**

Administrator i Podmiot Przetwarzający będą dalej zwani łącznie „**Stronami**", a każdy 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. Zważywszy, ze w celu realizacji obowiązków wynikających z umowy serwisowej Podmiot przetwarzający będzie miał dostęp do danych osobowych przetwarzanych w systemach objętych umową główną,
3. 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 (art. 28 ust. 3 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 B 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

1. 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 A 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:

otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2; oraz
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).
10. Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych, Podmiot Przetwarzający zobowiązuje się do stosowania szczególnych ograniczeń i dodatkowych zabezpieczeń technicznych i organizacyjnych, o których mowa w art. 32 RODO.

§ 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, na piśmie, odrębną umowę powierzenia przetwarzania danych osobowych (zwaną dalej umową podpowierzenia), w rozumieniu art. 28 ust. 4 RODO, z określeniem stosownego do Umowy cywilnoprawnej/Głównej celu, czasu i zakresu przetwarzania danych osobowych oraz rodzaju (kategorii) danych osobowych i kategorii osób, których te dane dotyczą;
   c) zawiera w umowie podpowierzenia zapis dotyczący uprawnień Administratora do przeprowadzenia audytu bezpieczeństwa (inspekcji) Podwykonawcy w zakresie bezpieczeństwa powierzonych mu danych osobowych w ramach umowy podpowierzenia;
   d) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów.
2. Podmiot przetwarzający bierze na siebie pełną odpowiedzialność za działania Podwykonawcy niezgodne z aktualnymi przepisami o ochronie danych osobowych lub postanowieniami Umowy cywilnoprawnej w zakresie ochrony danych osobowych lub Umowy powierzenia, a Stroną dla Administratora, w ewentualnych sporach wynikających z niewłaściwego wykonania przez Podwykonawcę tych umów, jest zawsze Podmiot Przetwarzający.
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 B 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 w sposób zapewniający poziom ochrony bezpieczeństwa odpowiadający ryzyku, zgodnie z art. 32 RODO.
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) ogólny opis naruszenia tj.: jak doszło do naruszenia ochrony danych osobowych (np. czy naruszenie było zamierzone czy też przypadkowe)
   b) opis charakteru 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 oraz atrybutów bezpieczeństwa informacji, które naruszono: poufność, integralność, dostępność imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia ochrony danych
   c) możliwe konsekwencje naruszenia ochrony danych osobowych; oraz 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.

W przypadku pozyskania dodatkowych informacji w późniejszym czasie Podmiot Przetwarzający przekazuje je Administratorowi bez zbędnej zwłoki.

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.
8. Podmiot przetwarzający zobowiązany jest niezwłocznie, nie później jednak niż w terminie 3 dni od dnia stwierdzenia naruszenia, do usunięcia nieprawidłowości w przetwarzaniu danych, które były przyczyną naruszenia lub zostały stwierdzone przez Administratora.

§ 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. Administrator poinformuje Podmiot przetwarzający o terminie planowanego audytu oraz zakresie jego prowadzenia z przynajmniej 7 dniowym wyprzedzenie z wyjątkiem sytuacji, o których mowa w §5 ust. 5. Administrator może również upoważnić do przeprowadzenia audytu niezależnego audytora.
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.
3. Czynności kontrolne nie mogą prowadzić do ujawnienia Administratorowi danych osobowych nieobjętych niniejszą umową, w szczególności danych osobowych innych klientów Wykonawcy, lub prowadzić do obniżenia skuteczności przyjętych przez Wykonawcę środków technicznych i organizacyjnych w celu ochrony

danych osobowych przetwarzanych w jego organizacji bądź zagrażać lub prowadzić do obniżenia poziomu ich bezpieczeństwa.

4. W trakcie czynności kontrolnych Zamawiający nie będzie miał dostępu do informacji niejawnych, o których mowa w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Osoby prowadzące czynności kontrolne na polecenie Administratora złożą na wniosek Podmiotu przetwarzającego stosowne oświadczenie o zachowaniu poufności informacji wskazanych przez Wykonawcę i stanowiących tajemnicę przedsiębiorstwa.
5. Czynności audytowe odbywają się wyłącznie w obecności osoby wyznaczonej przez Wykonawcę
6. Czynności audytowe nie mogą utrudniać działalności Wykonawcy, w szczególności wykonywania obowiązków przez pracowników lub współpracowników Wykonawcy.

§ 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. Zamawiający jest uprawniony do rozwiązania wszystkich umów zawartych z Podmiotem Przetwarzającym, z których wynika konieczność przetwarzania danych osobowych, w przypadku gdy:
   1) Podmiot Przetwarzający poważnie lub uporczywie narusza obowiązujące przepisy o ochronie danych osobowych albo postanowienia Umowy Głównej (cywilnoprawnej) lub Umowy powierzenia w zakresie ochrony danych osobowych;
   2) Podmiot Przetwarzający nie stosuje się do wiążącej decyzji właściwego organu nadzorczego lub orzeczenia sądu, dotyczących jego obowiązków wynikających z przepisów o ochronie danych osobowych lub postanowień Umowy Głównej (cywilnoprawnej) lub Umowy powierzenia.
3. Rozwiązanie, o którym mowa w ust. 1, może nastąpić:
   a) ze skutkiem natychmiastowym, w przypadku rażącego lub powtarzającego się naruszenia;
   b) po bezskutecznym upływie 5 dni od dnia doręczenia Podmiotowi Przetwarzającemu zawiadomienia o stwierdzonych nieprawidłowościach, jeżeli nie zostaną one usunięte w tym terminie.
4. Podmiot Przetwarzający zobowiązany jest do niezwłocznego usunięcia stwierdzonych nieprawidłowości w zakresie przetwarzania danych osobowych oraz przekazania Administratorowi pisemnego potwierdzenia ich usunięcia.
5. 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.
6. W przypadku rozwiązania Umowy w trybie ust. 2 wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
7. 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:

Rodzaje danych osobowych (np. imię, nazwisko, adres, numer PESEL, numer telefonu, e-mail, adres IP, dane o stanie zdrowia)	a) imię i nazwisko, nr PESEL, adres zamieszkania, adres e-mail, nr telefonu kontaktowego, data urodzenia, płeć, ID użytkownika systemu, b) Dane szczególnej kategorii: dane dotyczące zdrowia zawarte w dokumentacji z systemu PACS (opisy badań diagnostycznych) oraz bazach danych systemów objętych wsparciem
Kategorie osób, których dane osobowe dotyczą (np. pracownicy, dostawcy, pacjenci, kontrahenci, klienci)	Pacjenci, pracownicy
Zakres przetwarzania danych osobowych (czynności dokonywane na powierzonych danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, udostępnianie, zmienianie, usuwanie	porządkowanie, przeglądanie,
Charakter przetwarzania (np. systematyczny/sporadyczny)	sporadyczny
Cel przetwarzania (np. wykonanie umowy z dnia...)	Wykonanie umowy nr ..... z dnia ..... r.
Czas przetwarzania (np. *okres obowiązywania umowy z dnia...)*	Okres obowiązywania umowy nr ..... *od* ..... *r. do* ..... *r.*

Załącznik nr 3b – Podwykonawcy zatwierdzeni przez Administratora

Lp.	Nazwa	Adres	NIP
1.			
2.			
3.			

1. Zabezpieczenia organizacyjne i bezpieczeństwo fizyczne obszarów przetwarzania.

1.1. Wykonawca zapewnia, że spełnia wymagania określone w umowie powierzenia przetwarzania w szczególności wymagania, o których mowa w art. 28, 29, 30, 32 RODO.

1.2. Wykonawca oświadcza, że:

a) organizuje cykliczne szkolenia dla pracowników/współpracowników z zasad bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych;

b) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;

c) stosuje politykę czystego biurka oraz czystego ekranu (blokowanie komputerów przy pustych stanowiskach, niepozostawanie dokumentacji na biurkach, zamykanie szafek z dokumentacją, np..);

d) realizuje regularne audyty/kontrole bezpieczeństwa przetwarzania informacji;

e) wdrożył skuteczny proces zgłaszania oraz obsługi zdarzeń/incydentów związanych z naruszeniem bezpieczeństwa informacji w tym naruszeniem ochrony danych osobowych

f) zidentyfikował krytyczne procesy i usługi oraz opracowano dla nich plany ciągłości działania, oraz plany awaryjne w celu zapewnia zdolności do szybkiego przywrócenia dostępności danych wrażliwych i dostępu do nich, i usług krytycznych w razie incydentu fizycznego lub technicznego;

1.3. Dostęp do pomieszczeń, w których przechowywane są dane podlegające ochronie (dane osobowe, inne informacje o charakterze poufnym), mają tylko osoby do tego upoważnione. Dostęp jest objęty systemem kontroli dostępu. Wykonawca posiada stosowne procedury oraz zabezpieczenia techniczne w tym zakresie i jest w stanie wykazać ich stosowanie.

1.4. Wykonawca wdrożył zasady bezpiecznej pracy zdalnej i zapewnia, że:

a) wykonywanie pracy zdalnej odbywa się wyłącznie z miejsc zapewniających ochronę przed dostępem osób nieuprawnionych w sposób uniemożliwiający osobom trzecim wglądu w dane (np. przez zabezpieczenie stanowiska pracy przed dostępem osób postronnych),

b) urządzenia służbowe są zabezpieczonych hasłem, szyfrowaniem dysku oraz automatyczną blokadą ekranu po okresie bezczynności,

c) obowiązuje zakaz korzystania z niezabezpieczonych sieci publicznych,

d) obowiązuje zakaz drukowania i przechowywania dokumentów zawierających dane osobowe lub informacje poufne poza kontrolowanym środowiskiem biurowym.

1.5. W przypadku pracy zdalnej Wykonawca prowadzi ewidencję osób uprawnionych do pracy zdalnej z danymi Administratora danych oraz okresowo weryfikuje zgodność środowiska pracy z wymogami bezpieczeństwa.

2. Infrastruktura teleinformatyczna Zamawiającego objęta usługą określoną w umowie (urządzenia/systemy).

2.1. Wykonawca zapewnia, że systemy objęte Umową, na których przetwarzane są dane osobowe, są zabezpieczone przed dostępem osób nieupoważnionych oraz przed działaniem szkodliwego oprogramowania w zakresie elementów pozostających pod administracją lub kontrolą Wykonawcy albo konfigurowanych przez Wykonawcę w ramach realizacji Umowy, o ile producent tych systemów tego nie zabrania i jest to technologicznie możliwe. W zakresie elementów infrastruktury pozostających poza administracją Wykonawcy (w tym w szczególności warstwy wirtualizacji oraz systemów operacyjnych), Wykonawca przekazuje wymagania i zalecenia konfiguracyjne oraz współdziała przy ich wdrożeniu. Wykonawca zobowiązuje się zabezpieczyć dane przetwarzane w systemie oraz konfigurację tego systemu przed utratą, nieuprawnioną modyfikacją oraz ich ujawnieniem osobom nieupoważnionym.

2.2. Wykonawca zapewnia, że dostęp do systemu informatycznego, objętego usługą określoną w umowie, realizowany przez Wykonawcę, będzie spełniał wymagania określone dla infrastruktury Wykonawcy (z uwzględnieniem kont administratorskich na serwisowanych urządzeniach/systemach) o ile jest to możliwe technologicznie, a producent urządzeń tego nie zabrania.

2.3. W przypadku dokonywania istotnych zmian w systemie objętym Umową (np. zmiany konfiguracji) mogących powodować powstanie błędów lub utratę danych osobowych przetwarzanych w systemie, Wykonawca zobowiązany jest do zapewnienia kopii bezpieczeństwa przed podjęciem takich czynności, a w przypadku wyrobów medycznych - do uzyskania od Administratora danych potwierdzenia poprawności przesłania danych z urządzenia do systemu dziedzinowego Administratora danych.

2.4. W ramach zapewnienia bezpieczeństwa serwisowanych systemów Zamawiającego objętych umową Wykonawca oświadcza, że:

a) dokłada wszelkich starań, aby serwisowane systemy Zamawiającego objęte Umową, w tym komponenty dostarczone, skonfigurowane lub utrzymywane przez Wykonawcę w ramach realizacji Umowy, były odpowiednio zabezpieczone i funkcjonowały w sposób uniemożliwiający wyciek danych oraz dostęp osób nieuprawnionych,

b) ma obowiązek usuwania wykrytych luk i podatności bezpieczeństwa w komponentach serwisowanych systemów Zamawiającego objętych Umową, w zakresie pozostającym po stronie Wykonawcy.

c) zobowiązuje się niezwłocznie informować Administratora danych o wykrytych lukach w zabezpieczeniach i podatnościach dotyczących serwisowanych systemów Zamawiającego objętych Umową, które mogą zakłócić ciągłość działania Administratora danych lub mogą mieć wpływ na integralność, poufność i dostępność przetwarzanych danych.

3. Wykonawca i jego infrastruktura wykorzystywana do świadczenia usługi.

3.1. Wykonawca przekaże Zamawiającemu listę serwisantów wykonujących czynności serwisowe dotyczące systemów objętych Umową oraz dostarczy podpisane przez te osoby oświadczenia o zachowaniu poufności (**Załącznik nr 5**);

3.2. Wykonawca prowadzi rejestr zasobów informatycznych, które są wykorzystywane do świadczenia usługi (sprzęt, oprogramowanie, sieć) oraz monitoruje ich wykorzystanie. Dla tych zasobów Wykonawca oszacował ryzyko w kontekście bezpieczeństwa informacji oraz zastosował adekwatne zabezpieczenia techniczne i organizacyjne mające minimalizować ryzyko;

3.3. Wykonawca wdrożył system zarządzania systemem kontroli dostępu, który umożliwia przydzielanie, modyfikację oraz usuwanie uprawnień dostępu dla poszczególnych pracowników Wykonawcy do infrastruktury, w której odbywa się przetwarzanie danych osobowych (pomieszczenia, urządzenia, oprogramowanie, sieć), lub z której możliwy jest dostęp do zasobów Administratora danych. W szczególności Wykonawca zapewnia, że:

3.4. stosuje unikatowe nazwy użytkowników oraz politykę haseł zgodną z dobrymi praktykami. Poprzez dobre praktyki rozumie się co najmniej: stosowanie unikatowych identyfikatorów użytkowników, zakaz kont współdzielonych, stosowanie haseł o odpowiedniej złożoności i minimalnej długości, ograniczanie liczby nieudanych prób logowania, bezpieczne przechowywanie haseł, okresowy przegląd uprawnień oraz stosowanie MFA dla dostępu uprzywilejowanego i zdalnego, o ile jest to technologicznie możliwe. Jednocześnie Zamawiający dopuszcza, aby szczegółowe parametry polityki haseł wynikały z polityk bezpieczeństwa Wykonawcy, pod warunkiem, że zapewniają poziom bezpieczeństwa nie niższy niż wskazany powyżej.

3.5. dostęp do powierzonych danych osobowych przetwarzanych w serwisowanych systemach oraz infrastrukturze Wykonawcy objętych umową będą miały jedynie osoby posiadające uprawnienia do serwisowania tych systemów oraz posiadające upoważnienia do przetwarzania danych osobowych. Wykonawca posiada w tym zakresie stosowne procedury i jest w stanie wykazać ich stosowanie,

3.6. wykorzystywane urządzenia i systemy mobilne są zarejestrowane i przed dopuszczeniem do wykorzystania są autoryzowane, podlegają kontroli dostępu na takim samym poziomie jak pozostałe urządzenia i zapewnia, że infrastruktura informatyczna (urządzenia, oprogramowanie, transmisja danych w sieci) jest zabezpieczona przed dostępem osób nieupoważnionych oraz przed działaniem szkodliwego oprogramowania;

3.7. wszystkie urządzenia mobilne wykorzystywane do świadczenia usług w ramach Umowy podlegają szyfrowaniu przed ich dopuszczeniem do użytkownika;

3.8. W ramach zapewnienia bezpieczeństwa urządzeń/systemów wykorzystywanych do świadczenia usługi Wykonawca oświadcza, że:

a) dokłada wszelkich starań, aby urządzenia/systemy wykorzystywane do świadczenia usługi były odpowiednio zabezpieczone i funkcjonowały w sposób uniemożliwiający wyciek danych oraz dostęp osób nieuprawnionych;

b) ma obowiązek usuwania wykrytych luk i podatności bezpieczeństwa urządzeniach/systemach wykorzystywanych do świadczenia usługi;

c) zobowiązuje się niezwłocznie informować Administratora danych o wykrytych lukach w zabezpieczeniach i podatnościach dotyczących urządzeń/systemów Wykonawcy wykorzystywanych do świadczenia usługi w ramach Umowy, które mogą zakłócić ciągłość działania Administratora danych lub mogą mieć wpływ na integralność, poufność i dostępność przetwarzanych danych, oraz przedstawić rekomendacje minimalizujące ich negatywne skutki do czasu ich usunięcia;

d) zapewnia, że zarządzanie uprawnieniami w systemach wykorzystywanych do realizacji Umowy jest sformalizowane i udokumentowane;

e) elementy (urządzenia, systemy, oprogramowanie) wykorzystywane przez Wykonawcę do świadczenia usługi, pozostające pod jego administracją i kontrolą, podlegają aktualizacjom oraz zmianom konfiguracji w sposób planowany i kontrolowany, w oparciu o ocenę ryzyka i zalecenia producenta, z uwzględnieniem kompatybilności oraz wpływu na ciągłość świadczenia usługi; zmiany mogące wpływać na dostępność, integralność lub poufność danych bądź ciągłość świadczenia usługi są realizowane zgodnie z uzgodnionym z Zamawiającym procesem zarządzania zmianą.

3.9. Wykonawca stosuje narzędzia do wykrywania i reagowania na podejrzane aktywności urządzeń końcowych wykorzystywanych do świadczenia usługi;

3.10. Wykonawca identyfikuje podatności systemów informatycznych wykorzystywanych do świadczenia usługi oraz wdrożył proces zarządzania podatnościami technicznymi;

3.11. Do uwierzytelniania i identyfikacji użytkowników w systemach Wykonawcy wykorzystywanych do realizacji Umowy stosowane są mechanizmy adekwatne do ryzyka, zapewniające rozliczalność i ochronę przed nieuprawnionym dostępem.

4. Konta uprzywilejowane

4.1. Wykonawca zobowiązuje się do wdrożenia właściwej polityki haseł oraz zasad zarządzania hasłami kont uprzywilejowanych (administratorskich) w celu zapobiegania nieuprawnionemu dostępowi i nieautoryzowanym zmianom konfiguracyjnym systemów/urządzeń wykorzystywanych do świadczenia usługi, w tym do przetwarzania danych osobowych powierzonych do przetwarzania.

5. Ochrona podsieci

5.1. Wykonawca zapewnia, że komponenty wykorzystywane przez niego w ramach przydzielonego segmentu/VLAN generują wyłącznie ruch niezbędny do realizacji Umowy, zgodny z uzgodnioną z Zamawiającym macierzą połączeń oraz że transmisja danych odbywa się z wykorzystaniem mechanizmów zapewniających poufność i integralność (np. szyfrowanie) w zakresie, w jakim jest to technicznie możliwe dla danego systemu;

5.2. Dla uruchomienia przez Wykonawcę transmisji danych z urządzenia/systemu innym medium niż sieć kablowa Ethernet LAN (np. WI-FI, bluetooth lub GSM) wymagana jest pisemna zgoda Administratora danych. W przypadku planowania uruchomienia takiej transmisji Wykonawca zobowiązany jest do przedstawienia do akceptacji Administratorowi danych oceny skutków dla ochrony danych przesyłanych w taki sposób.

6. Nośniki danych i kopie danych.

6.1. Wykonawca zapewnia, że wdrożył procedury zarządzania nośnikami danych (np. DVD, pendrive, dysk zewnętrzny) oraz że podlegają one szyfrowaniu przed przekazaniem ich do użytku.

6.2. Wykonawca zapewnia, że ma wdrożone odpowiednie polityki/procedury dotyczące zarządzania nośnikami informacji (np. dyski HDD, SSD), na których są przetwarzane powierzone do przetwarzania dane osobowe i jest w stanie wykazać, że:

a) przed sprzedażą, przekazaniem, zakończeniem eksploatacji lub utylizacją przez Wykonawcę urządzeń/nośników danych pozostających pod jego administracją i kontrolą, na których w związku z realizacją Umowy mogły zostać utrwalone dane Zamawiającego, Wykonawca przeprowadza trwałe usunięcie danych (np. poprzez głębokie formatowanie lub inną skuteczną metodę uniemożliwiającą odtworzenie danych),

b) w przypadku braku możliwości wykonania procedury, o której mowa w lit. a), Wykonawca przeprowadza fizyczne zniszczenie nośnika danych w sposób skuteczny i nieodwracalny.

6.3. Wykonawca zapewnia, że nie będzie wykonywał, na zasobach nie należących do Administratora, danych kopii powierzonych do przetwarzania danych osobowych bez uprzednio wydanej pisemnej zgody Zamawiającego odrębnej dla każdej planowanej kopii danych. Wykonawca zapewnia, że kopia danych zostanie skutecznie, tj. w sposób nieodwracalny usunięta z zasobów Wykonawcy po zakończeniu czynności serwisowej, dla której wykonanie kopii danych było niezbędne. Z czynności tej Wykonawca sporządza protokół zawierający opis metodyki usunięcia danych. Protokoły te są przekazywane Administratorowi danych w raporcie okresowym, nie rzadziej niż raz w roku. Na żądanie Administratora danych Wykonawca udostępni protokół dotyczący wskazanej kopii danych/czynności serwisowej.

6.4. Przed uruchomieniem produkcyjnym (zasileniem systemu informatycznego danymi osobowymi i podłączenie do infrastruktury Zamawiającego) Wykonawca zobowiązany jest przedstawić Zamawiającemu do akceptacji konfigurację systemu, serwerów i komputerów oraz stosowane zabezpieczenia. Wykonawca ma obowiązek weryfikacji zastosowanej konfiguracji i zabezpieczeń

przez dwie niezależne osoby (pracownicy Wykonawcy). Zasilenie systemu oraz uruchomienie integracji z systemami dziedzinowymi może nastąpić po uzyskaniu od Zamawiającego zatwierdzenia konfiguracji systemów i urządzeń. Zamawiający w porozumieniu z Wykonawcą może przeprowadzić testy penetracyjne wdrażanego systemu przed zasileniem systemu danymi osobowymi.

6.5. Nośniki papierowe zawierające informacje poufne są niszczone w sposób uniemożliwiający odczyt informacji.

7. Licencje oraz integracje.

7.1. Wykonawca zapewnia, że możliwa jest pełna integracja pomiędzy systemem, którego dotyczy usługa (zgodnie z wymaganiami dokumentacji przetargowej), a właściwym systemem dziedzinowym Administratora danych umożliwiająca przesyłanie i odbierania komunikatów za pośrednictwem interfejsu TCP-IP oraz protokołu HL7, a w przypadku dokumentów protokołem HL7CDA. Jeżeli dla danego systemu/urządzenia w dokumentacji przetargowej przewidziano inny standard lub sposób integracji, integracja będzie realizowana zgodnie z tym standardem/sposobem (np. poprzez usługi sieciowe/API). Urządzenie zapewnia poprawną obsługę polskich znaków.

7.2. Licencje do integracji systemów dostarczone zostają na warunkach określonych w Umowie.

7.3. Z chwilą dostarczenia licencji Wykonawca zapewnia konfigurację, podłączenie oraz integrację systemu z właściwym systemem dziedzinowym Administratora danych.

8. Zdalny połączenie serwisowe systemów/urządzeń.

8.1. W sytuacji, gdy Zamawiający dopuszcza usługę zdalnego serwisu realizowaną za pośrednictwem sieci publicznej Internet, Wykonawca zapewnia, że podczas zdalnego serwisu urządzeń i systemów objętych Umową komunikacja (przesyłanie danych) pomiędzy systemem teleinformatycznym Zamawiającego, a systemem teleinformatycznym Wykonawcy odbywa się w sposób bezpieczny i jest szyfrowana (silne protokoły szyfrujące).

8.2. Przydzielenie zdalnego dostępu dla Wykonawcy będzie się odbywało zgodnie z zasadami obowiązującymi u Zamawiającego (indywidualne konta VPN dla serwisantów). Wykonawca przekaże z zachowaniem formy pisemnej wykaz osób uprawnionych do zestawienia połączenia zdalnego pomiędzy systemami teleinformatycznymi Zamawiającego, a systemem teleinformatycznym Wykonawcy. Sposób realizacji połączenia będzie uzgodniony z Działem Informatyki Zamawiającego.

8.3. Dane uwierzytelniające do logowania (systemów/urządzenia, zaszyfrowane pliki) będą odbierane osobiście przez osoby do tego upoważnione lub przekazywane SMS na wskazane w Umowie numery telefonów.

8.4. Wykonawca może wnioskować o dane logowania tylko i wyłącznie dla osób upoważnionych do przetwarzania danych osobowych powierzonych do przetwarzania na potrzeby należytej realizacji Umowy.

8.5. Wykonawca zapewnia, że nie będzie eksportował powierzonych do przetwarzania danych do Państw trzecich niespełniających wymagań, o których mowa w art. 45 ust.1 rozporządzenia 2016/679. Wykonawca zapewnia również, że połączenia zdalne do serwisowanych systemów i urządzeń nie będą realizowane z terytorium państwa trzeciego niespełniającego postanowień, o których mowa w art. 45 ust.1 rozporządzenia 2016/679 oraz że nie umożliwi transmisji danych osobowych do takiego państwa trzeciego.

8.6. Zabrania się Wykonawcy przekazywania danych logowania (login lub hasło) innym osobom niż osoby wskazane do realizacji Umowy.

8.7. Zdalny dostęp udostępnia się do realizacji usług wynikających z Umowy.

8.8. Korzystając ze Zdalnego Dostępu Wykonawca:

a) będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji Umowy;

b) nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji Umowy.

8.9. Na wezwanie Wykonawcy Zamawiający przekaże osobie realizującej prace wynikające z postanowień Umowy identyfikator użytkownika (login) wraz z hasłem dostępu oraz innymi parametrami niezbędnymi do zestawienia zdalnego połączenia. Hasło będzie miało charakter hasła startowego i będzie podlegało zmianie przy pierwszym logowaniu, zgodnie z zasadami obowiązującymi u Zamawiającego. Hasło zostanie przekazane bezpiecznym kanałem komunikacyjnym ustalonym przez strony. Użytkownicy po stronie Wykonawcy zobowiązują się do nieudostępniania tych identyfikatorów i haseł innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji Umowy.

8.10. W związku z realizacją Umowy w odniesieniu do infrastruktury Zamawiającego Wykonawcy zabrania się:

a) zmiany przyznanych adresów IP bez uprzedniego uzgodnienia z Zamawiającym,
b) rozdzielania sygnału na inne urządzenia niż określony w umowie (np. stosowanie routera itp.),
c) jakichkolwiek samowolnych zmian w infrastrukturze telekomunikacyjnej Zamawiającego,
d) dokonywania przeciążenia sieci teleinformatycznej Zamawiającego,
e) rozsyłania niechcianej poczty (SPAM),
f) używania bez zgody Zamawiającego niedozwolonych narzędzi sieciowych, takich jak sniffery, skanery portów, exploity,
g) wykorzystywania infrastruktury teleinformatycznej Zamawiającego w celu uruchamiania serwisów świadczących usługi komercyjne,
h) rozpowszechniania informacji sprzecznych z obowiązującym prawem oraz naruszających w jakikolwiek sposób uczucia religijne lub normy społeczne i obyczajowe,
i) świadczenia usług telekomunikacyjnych osobom trzecim, o ile wiążą się one z tranzytem informacji przez infrastrukturę Zamawiającego,
j) prowadzenia jakichkolwiek działań, które mogą powodować zakłócenia w działaniu infrastruktury Zamawiającego bez uprzednio uzyskanej zgody Zamawiającego,
k) podejmowania jakichkolwiek działań, które mogą uszkodzić infrastrukturę Zamawiającego, za pomocą której świadczona jest usługa lub mogących zakłócić poprawne funkcjonowanie systemów służących udostępnianiu i monitorowaniu usługi oraz urządzeń i łączy przeznaczonych do przekazywania informacji na odległość, za pomocą których świadczona jest Usługa,
l) dokonywania nieuzgodnionych z Zamawiającym napraw i zmian (w tym również instalacji oprogramowania i urządzeń sieciowych) w infrastrukturze telekomunikacyjnej Zamawiającego,
m) kierować do infrastruktury Zamawiającego ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych,
n) odmowy dostępu do infrastruktury Zamawiającego, w celu przeprowadzenia czynności kontrolnych, konserwacji lub naprawy,
o) wykorzystywania udostępnionej przez Zamawiającego infrastruktury niezgodnie z przepisami prawa lub niezgodnie z zawartą Umową,
p) uzyskiwania lub podejmowania prób uzyskania informacji z sieci teleinformatycznej Zamawiającego przy użyciu jakiejkolwiek metody, która nie została wyraźnie dopuszczona przez Zamawiającego,
q) przechwytywania, badania lub w inny sposób analizowania jakiegokolwiek komunikacyjnego protokołu używanego przez Zamawiającego, zarówno poprzez analizator sieci, program przechwytujący (sniffer) lub inne urządzenie bez uprzednio uzyskanej zgody Zamawiającego,
r) podejmowania działań, które nie są niezbędne do realizacji zawartych z Zamawiającym Umów.

9. Udostępnianie fragmentów baz danych i kopii danych.

9.1. Udostępnienie fragmentu bazy danych przez Administratora danych lub pobranie bazy danych przez Wykonawcę odbywa się na następujących zasadach:

a) Wykonawca zobowiązany jest zwrócić się do Administratora danych z uzasadnieniem merytorycznym pozyskania bazy danych do celów analizy zgłoszenia serwisowego i musi wykazać niezbędność oraz adekwatność takiej czynności z zachowaniem formy pisemnej,
b) Przed wykonaniem czynności pozyskania fragmentu bazy danych Wykonawca musi uzyskać zgodę Administratora danych wydanej z zachowaniem formy pisemnej,
c) niezwłocznie po zakończonej analizie pobranych danych, a jeżeli jest to uzasadnione koniecznością weryfikacji skuteczności wdrożonego rozwiązania, niezwłocznie po zakończeniu tej weryfikacji, jednak nie później niż w terminie 7 dni od dnia wdrożenia rozwiązania lub zamknięcia zgłoszenia serwisowego (w zależności od tego, które zdarzenie nastąpi później), Wykonawca zobowiązany jest do skutecznego i nieodwracalnego usunięcia danych ze swoich zasobów. Z czynności tej Wykonawca sporządza protokół zawierający opis metodyki usunięcia danych. Protokoły te są przekazywane Administratorowi danych w raporcie okresowym, nie rzadziej niż raz w roku. Na żądanie Administratora danych Wykonawca udostępni protokół dotyczący wskazanej kopii danych/czynności serwisowej.

d) Kopiowanie fragmentów baz danych jest możliwe jedynie na wskazane przez Administratora danych zasoby lub uzgodnione z Administratorem danych zasoby wskazane przez Wykonawcę.

9.2. Wykonawca wdrożył środki uniemożliwiające wykonanie nieautoryzowanych kopii danych o charakterze poufnym.

10. Obsługa zgłoszeń serwisowych i komunikacja z Administratorem danych.

10.1. Dopuszcza się obsługę zgłoszeń serwisowych z wykorzystaniem platformy helpdesku przy zapewnieniu bezpiecznego szyfrowania komunikacji z platformą.

10.2. Wykonawca zapewnia, że dane przetwarzane w systemie platformy helpdesku są zabezpieczone przed dostępem osób nieuprawnionych.

10.3. Dostęp do tych danych mają jedynie osobowy upoważnione, a dostęp realizowany jest jedynie przez tą platformę.

10.4. Wykonawca zapewnia, że zarządza retencją danych na platformie i zobowiązuje się z chwilą zakończenia umowy do usunięcia wszystkich danych osobowych zawartych w zamkniętych zgłoszeniach serwisowych (opisy, dokumenty itp.) po uzgodnieniu z Administratorem danych.

10.5. Nie dopuszcza się przesyłania drogą mailową zawartości zgłoszeń (np. opisy i analizy zgłoszeń, załączone pliki).

11. Podwykonawcy Wykonawcy.

11.1. Przed umożliwieniem Podwykonawcy dostępu do powierzonych danych Wykonawca zobowiązany jest uzyskać zatwierdzenie przez Administratora danych zgłoszonego Podwykonawcy z zastrzeżeniem formy pisemnej (Załącznik do umowy powierzenia przetwarzania danych).

11.2. Wykonawca oświadcza, że jego Podwykonawcy (mający dostęp do infrastruktury Administratora danych lub powierzonych danych osobowych) stosują poziom ochrony nie niższy niż określony przez Administratora danych oraz że ponosi odpowiedzialność za działania Podwykonawców jak za działania własne.

Oświadczam, że powyższe informacje są prawdziwe

.....

data i podpis osoby upoważnionej do złożenia oświadczenia w imieniu Wykonawcy

Załącznik nr 5 do Umowy nr
EI.273.10.III.2026

Oświadczenie o zachowaniu poufności

Ja, niżej podpisany .....

/Imiona, nazwisko/

zatrudnionym przez: ....., zwanego dalej Wykonawcą

realizując usługę na rzecz Wojewódzkiego Wielospecjalistycznego Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi, zwanego dalej Zamawiającym Ja, niżej podpisany, niniejszym oświadczam, że:

1. posiadam upoważnienie do przetwarzania danych osobowych, nadane przez Wykonawcę
2. zapoznałem się z przepisami dotyczącymi ochrony danych osobowych Rozporządzenia Parlamentu Europejskiego i Rady(UE) 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) zwanego dalej RODO, Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000 z późn. zm.) i zobowiązuję się do ich przestrzegania,

niniejszym zobowiązuję się do

- zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów i urządzeń tzn. informacji technicznych, technologicznych, prawnych organizacyjnych dotyczących urządzeń, systemów informatycznych/teleinformatycznych (np. urządzenia, wyroby medyczne, sprzęt informatyczny), uzyskanych w trakcie wykonywania umowy niezależnie od formy i źródła ich pozyskania,
- bezterminowego zachowania w tajemnicy wszelkich informacji dotyczących danych osobowych przetwarzanych w w/w urządzeniach i systemach oraz nieudostępniania ich treści osobom trzecim,
- wykorzystania w/w informacji jedynie w celach określonych ustaleniami umowy,
- zachowania w tajemnicy uzyskanych haseł dostępu do systemów informatycznych, urządzeń medycznych i pomieszczeń,
- zapewnienia bezpieczeństwa danych osobowych poprzez ich ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem,
- natychmiastowego zgłaszania przełożonemu oraz Pełnomocnikowi ds. Bezpieczeństwa w Szpitalu próby lub faktu naruszenia zabezpieczenia pomieszczenia, bezpieczeństwa zbioru, urządzenia lub systemu informatycznego, w którym przetwarzane są dane osobowe,
- niekopiowania lub niepowielania, ani w jakikolwiek inny sposób nierozpowszechniania jakiejkolwiek części w/w informacji,
- wykonywania poleceń Inspektora Ochrony Danych oraz innych przedstawicieli Szpitala odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobów ich zabezpieczenia w poufności.

Ponadto, oświadczam że:

- Znane mi są zasady odpowiedzialności prawnej za niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u administratora danych, kodeksu pracy, kodeksu karnego lub kodeksu cywilnego.

Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:

a. Administratorem Państwa danych osobowych jest Wojewódzkie Wielospecjalistyczne Centrum Onkologii Traumatologii im. M. Kopernika w Łodzi (93-513) z siedzibą przy ul. Pabianickiej 62, tel.: +48 42 689 50 00, e-mail: szpital@kopernik.lodz.pl

b. Wszelkie informacje i wątpliwości dotyczące przetwarzania Państwa danych przez Administratora można kierować do Inspektora Ochrony Danych pisemnie na adres administratora lub mailowo na adres iod@kopernik.lodz.pl
c. Państwa dane osobowe przetwarzane będą na podstawie art. 6 ust.1 lit. c) RODO w związku z realizacją umowy. W razie niepodania danych osobowych możliwa jest odmowa podpisania lub wykonanie umowy.
d. Dane osobowe 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).
e. Państwa dane osobowe będą przechowywane przez okres niezbędny do realizacji umowy oraz przez okres przechowywania dokumentacji wymagany przepisami powszechnie obowiązującego prawa.
f. Przysługuje Państwu prawo dostępu do treści swoich danych, prawo ich sprostowania i przysługuje prawo żądania: ich usunięcia, ograniczenia przetwarzania, przenoszenia oraz wniesienia sprzeciwu.
g. Państwa dane osobowe będą przetwarzane przez okres wskazany w art. 5 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach
h. Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.
i. Państwa dane zostały pozyskane od Wykonawcy.
j. Jeśli uznają Państwo, iż przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Państwu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Powyższe oświadczenie potwierdzam własnym podpisem

....., dnia .....
Miejscowość

.....
czytelny podpis osoby składającej oświadczenie

Załącznik nr 6 do umowy EI.273.10.III.2026
KLAUZULA INFORMACYJNA DLA OSÓB REPREZENTUJĄCYCH WYKONAWCĘ

Zgodnie z art. 13 oraz odpowiednio art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 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) zwanego dalej RODO, informujemy, iż:

a) Administratorem Państwa danych osobowych jest Wojewódzkie Wielospecjalistyczne Centrum Onkologii Traumatologii im. M. Kopernika w Łodzi (93-513) z siedzibą przy ul. Pabianickiej 62,tel.: +48 42 689 50 00, e-mail: szpital@kopernik.lodz.pl
b) Wszelkie informacje i wątpliwości dotyczące przetwarzania Państwa danych przez Administratora można kierować do Inspektora Ochrony Danych pisemnie na adres administratora lub mailowo na adres iod@kopernik.lodz.pl
c) Państwa dane osobowe przetwarzane będą na podstawie art. 6 ust.1 lit. b) i lit. c RODO w związku z realizacją umowy. W razie niepodania danych osobowych możliwa jest odmowa podpisania lub wykonania umowy z podmiotem będącym stroną umowy.
d) Dane osobowe 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) lub innym podmiotom, których udział w realizacji celów, o których mowa w ust. 3 powyżej jest niezbędne.
e) Państwa dane osobowe będą przechowywane przez okres niezbędny do realizacji umowy oraz przez okres przechowywania dokumentacji wymagany przepisami powszechnie obowiązującego prawa art. 5 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
f) Przysługuje Państwu prawo dostępu do treści swoich danych, prawo ich sprostowania i przysługuje prawo żądania: ich usunięcia, ograniczenia przetwarzania, przenoszenia oraz wniesienia sprzeciwu.
g) Jeśli uznają Państwo, iż przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Państwu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
h) Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.
i) Państwa dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowych.

Państwa dane zostały podane przez podmiot będący stroną zawartej umowy

Podpis Wykonawcy
.....

Testy akceptacyjne 2FA (SMS) – Portal Pacjenta

1. Cel

Potwierdzenie poprawnego działania uwierzytelniania dwuskładnikowego (2FA) z użyciem jednorazowego kodu SMS podczas logowania do Systemu.

2. Warunki wstępne

1. Dostęp do środowiska testowego lub produkcyjnego (zgodnie z ustaleniami Stron).
2. Dwa konta testowe:
   - Konto A – z poprawnym numerem telefonu i możliwością odbioru SMS,
   - Konto B – bez numeru telefonu lub z numerem niezweryfikowanym (test negatywny).
3. Aktywna integracja z bramką SMS.

3. Kryteria odbioru

1. Wszystkie testy oznaczone jako **Krytyczne** muszą zakończyć się wynikiem **PASS**.
2. Funkcjonalność uznaje się za wdrożoną, jeżeli 2FA działa w środowisku produkcyjnym oraz testy krytyczne zostały zaliczone i potwierdzone w protokole.

4. Przypadki testowe

ID	Test	Priorytet	Kroki (skrót)	Oczekiwany wynik	Wynik (PASS/FAIL)	Uwagi
T1	Logowanie z poprawnym OTP	Krytyczny	Login+hasło → odbierz SMS → wpisz OTP	Logowanie skuteczne		
T2	Błędny OTP	Krytyczny	Login+hasło → wpisz błędny OTP	Brak logowania, komunikat błędu		
T3	OTP wygasły	Krytyczny	Wygeneruj OTP → odczekaj → wpisz OTP	Brak logowania, możliwość wygenerowania nowego		
T4	Ponowne użycie OTP	Krytyczny	Zaloguj się OTP → wyloguj → spróbuj użyć tego samego OTP	Odmowa (OTP jednorazowy)		
T5	Limit prób/ blokada	Krytyczny	Wpisuj błędny OTP do limitu	Blokada lub odmowa dalszych prób zgodnie z ustawieniami		
T6	Ponowna wysyłka kodu (resend)	Ważny	Kliknij „Wyślij ponownie"	Kod przychodzi, system ogranicza nadużycia (brak spamowania)		
T7	Konto bez numeru telefonu	Krytyczny	Login+hasło na koncie B	Brak możliwości przejścia 2FA bez spełnienia wymagań (brak obejścia)		
T8	Awaria wysyłki SMS	Ważny	Próba logowania przy braku wysyłki	Kontrolowany komunikat, brak logowania bez OTP		

* OTP – One-Time Password (jednorazowe hasło)

5. Potwierdzenie wykonania

Testy wykonano w dniu: _____ w środowisku: _____
Osoby wykonujące testy: _____

Podpis Zamawiającego: _____ Podpis Wykonawcy: _____