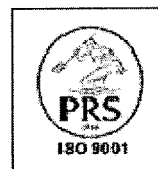




Wojewódzki Szpital Zespolony w Kielcach

25-736 Kielce, ul. Grunwaldzka 45
tel: 41/36-71-301, fax: 41/34-50-623
e-mail: szpital@wszkielce.pl
www.wszkielce.pl



EZ/112/2025/RL

Kielce dn. 05.08.2025 r

Do wszystkich zainteresowanych

Dotyczy postępowania o udzielenia zamówienia publicznego prowadzonego w trybie podstawowym na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2024, poz. 1320). Przedmiotem zamówienia jest „**Usługa nadzoru autorskiego i świadczenie opieki serwisowej dla Zintegrowanego Systemu Informatycznego Amms/Infomedica Plus** część administracyjna dla potrzeb Wojewódzkiego Szpitala Zespolonego w Kielcach”

ODPOWIEDZI NA PYTANIA

Działając w oparciu o art. 284 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2024 r. poz. 1320), Zamawiający Wojewódzki Szpital Zespolony w Kielcach ul. Grunwaldzka 45 udostępnia odpowiedzi na zadane pytania:

Pytanie nr 1

Wykonawca zwraca się z wnioskiem o zmianę w § 2 PPU pkt 2 ppkt f) postanowienia w nw. brzmieniu:

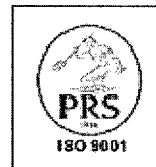
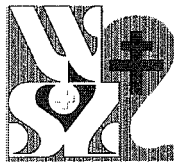
„Usługi serwisu, świadczone będą przez Wykonawcę w zakresie nieprzekraczającym 5 rdn miesięcznie, tj. 30 roboczogodzin miesięcznie, ~~gdzie w przypadku konsultacji zdalnych dzień pracy obejmuje 8 h roboczych, w przypadku wizyty na miejscu 6 h roboczych.~~ Limit obejmuje całość prac wykonanych przez Wykonawcę dla realizacji zgłoszeń lub zadań serwisowych zarówno w siedzibie Zamawiającego, Wykonawcy, Autoryzowanego Przedstawiciela Serwisowego Wykonawcy jak i poprzez połączenia zdalne realizowane przez ich personel.”

Odpowiedź: Zamawiający modyfikuje treść PPU § 2 ust. 2 pkt 2) f) który otrzymuje brzmienie:

„Usługi serwisu, świadczone będą przez Wykonawcę w zakresie nieprzekraczającym 5 rdn miesięcznie, tj. 30 roboczogodzin miesięcznie. Limit obejmuje całość prac wykonanych przez Wykonawcę dla realizacji zgłoszeń lub zadań serwisowych zarówno w siedzibie Zamawiającego, Wykonawcy, Autoryzowanego Przedstawiciela Serwisowego Wykonawcy jak i poprzez połączenia zdalne realizowane przez ich personel”.

Jednocześnie Zamawiający modyfikuje treść Załącznika nr 2 do SWZ - formularz asortymentowo cenowy pkt. 19, który otrzymuje brzmienie „Serwis oprogramowania aplikacyjnego (5rdn/miesięcznie) tj. 30 roboczogodzin miesięcznie”

Zmodyfikowany Załącznik nr 2 do SWZ- formularz asortymentowo- cenowy wraz ze Zmodyfikowanym Załącznikiem nr 3 do SWZ-projektowane postanowienia umowy zostaną udostępnione na stronie prowadzonego postępowania.



Pytanie nr 2

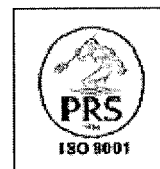
Wykonawca wnosi o dodanie do Umowy nw. definicji pojęć:

Błąd Zwykły Oprogramowania Aplikacyjnego	- niespowodowane przez użytkownika, niezgodne z dokumentacją, powtarzalne działanie Oprogramowania Aplikacyjnego, występujące w tym samym miejscu programu, na stacji roboczej skonfigurowanej zgodnie z zaleceniami producenta Oprogramowania Aplikacyjnego i prowadzące w każdym przypadku do otrzymania błędnych wyników jego działania, udokumentowane co najmniej poprzez opis ścieżki powtórzenia, zapisy logów systemowych i/lub zrzuty ekranów. Wszelkie uwagi związane z wyglądem, estetyką, ergonomią bądź przyzwyczajeniami Użytkownika (Zamawiającego) oraz uwagi dotyczące rozbudowy lub ograniczenia funkcjonalności nie są traktowane jako Błędy;
Błąd Krytyczny Oprogramowania Aplikacyjnego	- należy przez to rozumieć niezgodne z dokumentacją, powtarzalne działanie Oprogramowania Aplikacyjnego, w którym niemożliwie jest użytkowanie Oprogramowania Aplikacyjnego w zakresie jego Podstawowej Funkcjonalności (t.j. takiej, która dotyczy każdego użytkownika, występuje na każdej Stacji roboczej skonfigurowanej do pracy z danym modulem Oprogramowania Aplikacyjnego zgodnie z zaleceniami producenta Oprogramowania Aplikacyjnego w tym na każdej przeglądarce zalecanej i skonfigurowanej do pracy z Oprogramowaniem Aplikacyjnym zgodnie z zaleceniami producenta) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego;
Awaria	- nieoczekiwane zachowanie się Systemu Informatycznego, które wystąpiło w czasie jego pracy, skutkujące całkowitą niedostępnością Systemu Informatycznego lub nagłym spadkiem wydajności powodującym całkowitą niedostępność systemu.
Zgłoszenie Serwisowe	- należy przez to rozumieć zgłoszenie potrzeby Zamawiającego w zakresie realizacji zobowiązań zawartych w Umowie względem Zamawiającego, w obszarze czynności serwisowych, rejestrowane przez Zamawiającego w Systemie CHD;

**Wojewódzki Szpital Zespolony w Kielcach**

25-736 Kielce, ul. Grunwaldzka 45

tel: 41/36-71-301, fax: 41/34-50-623

e-mail: szpital@wszkielce.plwww.wszkielce.pl

Zadania Serwisowe	-	należy przez to rozumieć czynności serwisowe realizowane dla Zamawiającego, a związane z obsługą serwisową Zamawiającego, rejestrowane przez Wykonawcę lub jego Autoryzowanego Przedstawiciela Serwisowego w Systemie CHD;
Dzień Roboczy	-	należy przez to rozumieć każdy dzień od poniedziałku do piątku w godzinach 8:00 do 16:00, z wyłączeniem dni ustawowo wolnych od pracy;
Kierownik Projektu	-	należy przez to rozumieć osobę ze strony Wykonawcy odpowiedzialną za realizację Umowy;
Oprogramowanie Aplikacyjne	-	należy przez to rozumieć moduły oprogramowania AMMS PLUS/Infomedica PLUS oferowanego przez Wykonawcę, z których korzysta Zamawiający, będące przedmiotem Umowy, wskazane w Załączniku nr 1;
Oprogramowanie Bazodanowe	-	należy przez to rozumieć oprogramowanie bazodanowe Oracle, stanowiące podstawę działania bazy danych Systemu Informatycznego Wykonawcy, z których korzysta Zamawiający;
System Informatyczny	-	należy przez to rozumieć moduły Oprogramowania Aplikacyjnego, wymienione w Załączniku nr 1, dostarczanego przez Wykonawcę, wraz z platformami integracyjnymi, bazami danych (z wyłączeniem serwerów baz danych wraz z jego Oprogramowaniem Bazodanowym) oraz serwerami aplikacji i serwerami www, z którymi współpracuje Oprogramowanie Aplikacyjne;
Umowa	-	należy przez to rozumieć niniejszą umowę;
System CHD	-	System typu HelpDesk udostępniany przez Wykonawcę do rejestracji i obsługi zgłoszeń Zamawiającego i Wykonawcy oraz do rejestracji prac serwisowych wykonywanych przez Wykonawcę lub Autoryzowanego Przedstawiciela Serwisowego Wykonawcy, dostępny pod adresem.....;

Odpowiedź: Zamawiający wyraża zgodę na dodanie w treści umowy powyższych definicji.

Zamawiający dodaje w treści projektu umowy §15 o nazwie „Definicje”.

Dotychczasowy §15 „Postanowienia końcowe” staje się §16 i nie zmienia swojej treści.

Pytanie nr 3

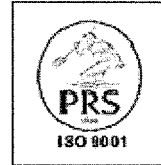
Wykonawca zwraca się z wnioskiem o wprowadzenie do § 6 PPU postanowienia w nw. brzmieniu:

„Zmiana stawki podatku od towarów i usług (VAT) w trakcie obowiązywania niniejszej Umowy, w odniesieniu do usług przewidzianych niniejszą Umową, skutkuje, z dniem wejścia w życie nowej stawki VAT, zmianą wynagrodzenia brutto należnego Wykonawcy i nie stanowi zmiany niniejszej Umowy, oraz nie wymaga aneksu do niniejszej Umowy”.

Dział Zamówień Publicznych

tel: 41/36-71-269

renata.lastowska@wszkielce.pl



Jednocześnie Wykonawca zwraca się z wnioskiem o usunięcie § 14 ust. 3 pkt. b) PPU:

Zgodnie z brzmieniem § 14 ust. 3 pkt. b) PPU zmiana wynagrodzenia brutto w razie zmiany stawki podatku VAT wymaga zmiany umowy.

Wykonawca informuje, że w chwili ustawowej zmiany stawki podatku VAT nie ma możliwości wystawić faktury za wykonanie przedmiotu zamówienia inaczej, niż zgodnie z obowiązującym prawem podatkowym.

Dostosowywania stosowanych w umowie stawek podatku VAT do wynikających z aktualnie obowiązujących przepisów prawa nie można uzależniać od woli stron, w związku z powyższym aneksowanie zmiany podatku VAT nie jest konieczne.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 4

Wykonawca w odniesieniu do § 8 PPU (Kary umowne) wnosi o dokonanie zmiany, poprzez modyfikację, iż Zamawiający będzie naliczał kary umowne od „wartości wynagrodzenia netto”.

Zważywszy, że odszkodowanie wypłaca się zawsze od kwoty netto (podatek VAT nie jest składnikiem wynagrodzenia wykonawcy) właściwą praktyką jest formułowanie zapisów dotyczących kar w oparciu o wynagrodzenie netto.

Zamawiający planuje naliczać kary od wartości umowy brutto, czyli również od pobranego do przekazania Skarbowi Państwa podatku VAT. Tymczasem, jeśli kara ma być proporcjonalna do wynagrodzenia Wykonawcy to powinna się odnosić do wartości netto, ponieważ podatek VAT nie jest wynagrodzeniem Wykonawcy, tylko podatkiem pobranym do odprowadzenia do urzędu skarbowego. Wykonawca nie zarabia na VATcie. VAT nie należy do Wykonawcy, tylko do budżetu państwa. Wynagrodzeniem Wykonawcy jest wyłącznie kwota netto.

Ponadto Wykonawca zwraca się z wnioskiem o wprowadzenie w § 5 ust. 1 i ust. 6 PPU podziału na wynagrodzenie brutto i netto.

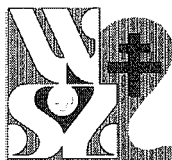
Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 5

Wykonawca wskazuje, że zgodnie z art. 484 § 2 KC: „Jeżeli zobowiązanie zostało w znacznej części wykonane, dłużnik może żądać zmniejszenia kary umownej; to samo dotyczy wypadku, gdy kara umowna jest rażąco wygórowana.”

Dokonując analizy wskazanego wzoru umowy, Wykonawca dochodzi do wniosku, że kary umowne są rażąco wygórowane. Mając na uwadze stanowisko judykatury, na karę powinna wpływać wartość wynagrodzenia i potencjalna szkoda. W wyroku z 11 października 2016 r. Sąd Apelacyjny w Warszawie (sygn. akt I ACa 1673/15) stwierdził, iż przy ocenie, czy „zastrzeżona kara umowna jest rażąco wygórowana nie wyklucza się uwzględnienia relacji między wysokością zastrzeżonej kary umownej

a wysokością wynagrodzenia należnego stronie zobowiązanej do zapłaty kary umownej. Za zasadnicze jednak kryterium tej oceny uznaje się stosunek wysokości zastrzeżonej kary umownej do wysokości szkody doznanej przez wierzyciela.”



Mając na uwadze wynagrodzenie oraz potencjalną szkodę i standardy obowiązujące na rynku IT, Wykonawca wnosi o zmianę wysokości kar określonych w § 8 ust. 1 pkt 2 według poniższego zestawienia:

„ 2. Wykonawca zapłaci kary umowne Zamawiającemu:

- za odstąpienie od umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy - w wysokości **10%** wynagrodzenia brutto, o którym mowa w § 5 ust. 6,
- za zwłokę realizacji postanowień umownych w stosunku do terminów określonych w umowie umowy lub ustalonych z Zamawiającym w wysokości **1000,00 zł** za dzień zwłoki,
- za zwłokę w przedłożeniu dokumentów potwierdzających zatrudnienie na umowę o pracę osób o których mowa w § 2 ust 6 na wezwanie Zamawiającego w wysokości **300,00 zł** za każdy dzień zwłoki. ”

na nw. brzmienie, tj.:

2. „Wykonawca zapłaci kary umowne Zamawiającemu:

- za odstąpienie od umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy - w wysokości **10%** wynagrodzenia netto, o którym mowa w § 5 ust. 6,
- za zwłokę realizacji postanowień umownych w stosunku do terminów określonych w umowie umowy lub ustalonych z Zamawiającym w wysokości **0,1%** za dzień zwłoki, jednak nie więcej niż **10%** wynagrodzenia miesięcznego za każdy przypadek,
- za zwłokę w przedłożeniu dokumentów potwierdzających zatrudnienie na umowę o pracę osób o których mowa w § 2 ust 6 na wezwanie Zamawiającego w wysokości **300,00 zł** za każdy dzień zwłoki. ”

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 6

Wykonawca zwraca się z pytaniem czy Zamawiający dopuszcza możliwość modyfikacji zapisów § 8 ust. 2 PPU w poniższy sposób:

„ Łączna maksymalna wysokość kar umownych nie może przekroczyć 20% wynagrodzenia netto, o którym mowa w § 5 ust. 6 Umowy”.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 7

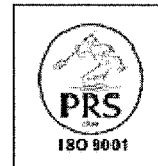
Wykonawca zwraca się z wnioskiem o wykreślenie ust. 3 § 8 PPU w brzmieniu:

„Zamawiający zastrzega sobie prawo potrącenia kar umownych z wynagrodzenia należnego Wykonawcy.

O potrąceniu Zamawiający zawiadomi Wykonawcę w formie pisemnej wraz z podaniem uzasadnienia.”

Wykonawca wskazuje, że powszechnie obowiązujące przepisy prawa jasno wskazują przesłanki dochodzenia roszczeń, a zatem powyższy zapis jest nadmiarowy. Wykonawca oczekuje aby mieć możliwość „przedyskutowania” potencjalnie naliczonych kar umownych. Wyraźne postanowienie, że Zamawiający nie może potrącać kar z wynagrodzenia, daje mu taką możliwość.

Odpowiedź: Zamawiający odmawia dokonania zmiany.



Pytanie nr 8

Wykonawca w odniesieniu do § 8 ust. 4 PPU wnosi o jego zmodyfikowanie poprzez nadanie mu nw. brzmienia:

„Jeżeli kary umowne przewidziane w niniejszym paragrafie nie pokryją szkody faktycznie poniesionej, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego, z zastrzeżeniem, że całkowita odpowiedzialność odszkodowawcza Wykonawcy wynikająca z nienależytego wykonania przedmiotu Umowy ogranicza się do rzeczywistej straty Zamawiającego, bez utraconych korzyści, z jednoczesnym ograniczeniem do równowartości 100% wynagrodzenia netto, o którym mowa w § 5 ust. 6 Umowy”.

Zgodnie z obowiązującym standardem opublikowanym przez Urząd Zamówień Publicznych „Analiza dobrych praktyk w zakresie realizacji umów IT, ze szczególnym uwzględnieniem specyfiki projektów informatycznych 7 Osi POIG”, w umowach IT odpowiedzialność stron jest ograniczana do szkody rzeczywistej. Jest to podyktowane potrzebą wyeliminowania sytuacji, w której strona będzie odpowiadała za trudne do skwantyfikowania utracone korzyści drugiej strony.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 9

Wykonawca z uwagi na chęć wyeliminowania niepewności prawnej wnosi o dodanie do § 8 PPU dodatkowego ustępu w nw. brzmieniu:

„Zamawiający ma prawo naliczyć kare umowną w terminie do 90 dni od dnia zaistnienia przyczyn, stanowiących podstawę ich naliczenia. Po upływie tego terminu prawo do naliczenia kary, w oparciu o przyczyny stanowiące podstawę ich naliczenia, wygasa”.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 10

Mając na uwadze nierówne ukształtowanie praw i obowiązków Stron odnośnie możliwości odstąpienia od umowy, Wykonawca wnosi o zmianę § 10 ust. 2 pkt 1 ppkt c) PPU poprzez nadanie mu nw. brzmienia:

„Wykonawca jest w zwłoce rozpoczęciu realizacji usługi ponad 14 dni od upływu wyznaczonych terminów

i pomimo wyznaczenia dodatkowego terminu nie realizuje usługi zgodnie z umową,”

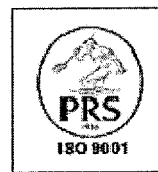
Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 11

Wykonawca wnosi o wykreślenie niejasnego interpretacyjnie § 10 ust. 2 pkt 1) lit. e) PPU w nw. brzmieniu:

„Wykonawca trzykrotnie został ukarany za naruszenie tożsamyh obowiązków określonych w umowie w okresie trzech miesięcy świadczenia usługi”

Wykonawca w tym miejscu wskazuje, że postanowienie ww. kształcie pozostaje niejednoznaczne i nie pozwala na jasne określenie okoliczności w których istnieją podstawy do odstąpienia od umowy przez Zamawiającego.



W przypadku braku wykreślenia postanowienia w ww. kształcie Wykonawca wnosi o dokonanie jego wykładni przez Zamawiającego.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 12

Wykonawca w odniesieniu do brzmienia § 12 ust. 2 PPU (Prawa autorskie) wnosi o wskazanie w nw. postanowieniu aktualnego Dziennika Ustaw poprzez skorygowanie postanowienia w nw. sposób:

„Oprogramowanie Aplikacyjne, którego dotyczy niniejsza umowa jest chronione prawem autorskim wynikającym z przepisów Ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych

(t.j. Dz. U. z 2025 r. poz. 24 z późn. zm.). Zamawiający i Wykonawca zobowiązują się do respektowania tych praw niezależnie od powstałych okoliczności.”

Odpowiedź: Zamawiający modyfikuje § 12 ust. 2 PPU aktualny Dziennik Ustaw, Załącznika nr 3 do SWZ - projektowane postanowienia umowy o zamówienie publiczne.

Pytanie nr 13

Wykonawca wnosi o zmodyfikowanie brzmienia § 15 ust. 2 PPU poprzez nadanie mu nw. brzmienia:

„Wszelkie sprawy sporne wynikłe na tle realizacji niniejszej umowy strony będą starały się rozstrzygać polubownie. W razie braku porozumienia sprawy sporne rozstrzygać będzie właściwy sąd dla siedziby Wykonawcy”.

Odpowiedź: Zamawiający odmawia dokonania zmiany.

Pytanie nr 14

Wykonawca zwraca się do Zamawiającego z pytaniem czy Zamawiający przewiduje uregulowanie w umowie zasad przetwarzania danych osobowych ze wskazaniem podwykonawców uprawnionych do przetwarzania danych w toku wykonania przedmiotu Umowy.

Wykonawca wskazuje, że Zamawiający w § 15 ust. 3 PPU odnosi się do Umowy powierzenia przetwarzania danych osobowych. Wykonawca w tym miejscu wnosi o dodanie do Umowy w ramach odrębnej jednostki redakcyjnej nw. postanowień regulujących ochronę danych osobowych:

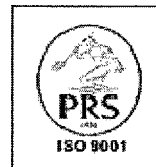
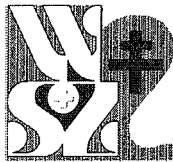
„ §

Ochrona danych osobowych

1. W związku z koniecznością wykonywania operacji przetwarzania danych osobowych, Zamawiający, na podstawie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (dalej : RODO) powierza Wykonawcy do przetwarzania dane osobowe w zakresie niezbędnym do prawidłowej realizacji niniejszej Umowy.

2. Pod pojęciami „dane osobowe” lub „dane” użytymi w Umowie, Strony rozumieją dane osobowe zdefiniowane w art. 4 pkt 1 RODO, których rodzaj i zakres zostały wskazane w Umowie.



3. Zamawiający oświadcza, że jest administratorem w rozumieniu art. 4 ust. 7 RODO, lub jest uprawniony, na mocy art. 28 ust. 2 RODO do dalszego powierzenia Wykonawcy przetwarzania danych osobowych.

4. Wykonawca oświadcza, że jest podmiotem przetwarzającym w rozumieniu art. 4 pkt 8 RODO i posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Wykonawca oświadcza, że znane mu są zasady przetwarzania danych osobowych wynikające z RODO.

5. Przetwarzanie odbywać się będzie w formie elektronicznej, poprzez wykonywanie wszystkich operacji przetwarzania uzasadnionych wykonywaniem usług objętych przedmiotem Umowy. Wykonawca jest uprawniony w szczególności do wykonywania następujących operacji przetwarzania: utrwalanie, porządkowanie/organizowanie, pobieranie, przysyłanie, przechowywanie, usuwanie oraz inne operacje, o ile okażą się niezbędne do prawidłowej realizacji Umowy.

6. Dostęp do powierzonych danych osobowych odbywać się będzie za pośrednictwem szyfrowanego łącza VPN, aktywowanego w związku z realizacją Umowy lub w innej, szyfrowanej formie ustalonej między Stronami.

7. Przetwarzanie będzie wykonywane w okresie realizacji Umowy i wszystkich zobowiązań z niej wynikających.

8. Uwzględniając charakter usług świadczonych na podstawie Umowy, stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Wykonawca zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych tak, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w szczególności zobowiązuje się do stosowania zabezpieczeń wskazanych w Załączniku nr do niniejszej Umowy.

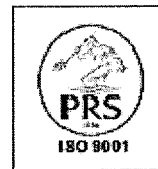
9. Przetwarzanie obejmować będzie rodzaje danych osobowych wskazane poniżej:

- 1) Dane identyfikacyjne,
- 2) Dane adresowe,
- 3) Dane dot. stanu zdrowia,
- 5) Dane kontaktowe,
- 6) Numery systemowe umożliwiające identyfikację,
- 7) Inne dane osobowe, związane z realizowanymi zadaniami Zamawiającego w szczególności informacje opisujące relacje Zamawiającego z Pacjentami, Pracownikami i Kontrahentami Zamawiającego.

10. Przetwarzanie danych będzie dotyczyć następujących kategorii osób:

- 1) Pracownicy i personel medyczny świadczący usługi dla Zamawiającego i osoby, z którymi wchodzić oni w interakcje społeczne,
- 2) Pacjenci Zamawiającego i osoby, z którymi wchodzić oni w interakcje społeczne
- 3) Kontrahenci Zamawiającego.

11. Dostęp do danych osobowych przydzielany jest w oparciu o zasadę minimalnych koniecznych uprawnień, tj. tylko uprawnień niezbędnych do wykonania czynności określonych w Umowie. Osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania tajemnicy.



12. Wykonawca przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Zamawiającego, przy czym Strony uzgadniają, że za udokumentowane polecenia uznaje się niniejszą Umowę oraz zadania i czynności zlecane do wykonania Wykonawcy w ramach Umowy.

13. Wykonawca będzie prowadził rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zawierający informacje wskazane w art. 30 ust. 2 RODO i na zasadach tam określonych.

14. Zamawiający wyraża ogólną zgodę na dalsze powierzenie przez Wykonawcę innemu przetwarzającemu (dalej: Inny Podmiot Przetwarzający), oraz Podwykonawcom, w drodze pisemnej umowy dalszego przetwarzania („Umowa podpowierzenia”), pod warunkiem uprzedniej akceptacji przez Zamawiającego lub braku jego sprzeciwu, który to sprzeciw Zamawiający może wyrazić w terminie 7 dni od dnia otrzymania stosownej informacji od Wykonawcy. Inny Podmiot Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych tak, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Strony przyjmują, iż wskazane w ust. 14 Inne Podmioty Przetwarzające są podmiotami, którym Wykonawca może powierzyć dalsze przetwarzanie danych osobowych i uzyskanie dodatkowej zgody Zamawiającego, o której mowa powyżej nie jest wymagane. Celem uniknięcia wątpliwości interpretacyjnych Strony zgodnie postanawiają, że osoby fizyczne współpracujące z Wykonawcą na podstawie umów cywilno-prawnych są traktowane jak personel Wykonawcy i nie stanowią Innych Podmiotów Przetwarzających. To samo dotyczy personelu Innego Podmiotu Przetwarzającego, o ile podmiot ten został zaakceptowany przez Zamawiającego.

15. Lista Innych Podmiotów Przetwarzających zaakceptowanych przez Zamawiającego:

1) **[należy uzupełnić]**

Podmiot ten realizuje na rzecz Wykonawcy usługi bieżącego wsparcia dla działalności Wykonawcy, [w szczególności usługi: wsparcia technicznego dla użytkowników, związane z utrzymaniem poczty, administrowania serwerami systemów i aplikacji wewnętrznych, kolokacji, tworzenia, wdrażania, administrowania zasad i narzędzi cyberbezpieczeństwa, administrowanie narzędziami i obsługa incydentów cyberbezpieczeństwa, monitorowania cyberbezpieczeństwa.

2) Podwykonawcy wskazani w § 4 ust. 1 Umowy.

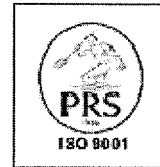
16. Wykonawca realizując zadania wynikające z Umowy i biorąc pod uwagę charakter świadczonych usług, w miarę możliwości udzieli pomocy Zamawiającemu w zakresie:

a) niezbędnego wsparcia w realizacji obowiązku odpowiadania na zapytania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO,

b) niezbędnego wsparcia w realizacji obowiązków wynikających z art. 32–36 RODO.

17. Wykonawca bezzwłocznie - nie później jednak niż w ciągu 48 godzin od jego wystąpienia - zgłosi na adres e-mail: **[należy uzupełnić]** lub **[należy uzupełnić]** Zamawiającemu każde naruszenie danych osobowych powierzonych niniejszą Umową którego będzie uczestnikiem.

18. Wykonawca po zakończeniu przetwarzania danych osobowych w związku z realizacją wszystkich zobowiązań wynikających z Umowy, niezwłocznie zwróci powierzone mu dane lub dokona ich usunięcia – adekwatnie do ustaleń z Zamawiającym. Czynności zwrotu i/lub usunięcia, każdorazowo winny zostać potwierdzone odpowiednio przez Strony.



19. Wykonawca zobowiązuje się udostępnić Zamawiającemu informacje niezbędne do wykazania spełnienia obowiązków określonych w artykule 28 RODO oraz umożliwić Zamawiającemu przeprowadzenie audytów w odniesieniu do danych przetwarzanych przez Wykonawcę w związku z realizacją przedmiotu Umowy.

20. Wykonawca oświadcza, iż na dzień zawarcia Umowy nie przekazuje danych osobowych powierzonych mu do przetwarzania do państw spoza EOG lub do organizacji międzynarodowych. W razie uwzględnienia przez Zamawiającego wniosku Wykonawcy o dodanie do treści Umowy w ramach odrębnej jednostki redakcyjnej postanowień regulujących zasady przetwarzania danych osobowych (Ochrona danych osobowych), Wykonawca wnosi o wykreślenie z PPU § 15 ust. 3 PPU, wskazującego na zawarcie pomiędzy Stronami odrębnej umowy powierzenia przetwarzania danych osobowych, celem uniknięcia podwójnego powierzenia przetwarzania danych osobowych i uniknięcia wątpliwości interpretacyjnych przy stosowaniu przepisów RODO. Jednocześnie Wykonawca wnosi o dodanie do Umowy Załącznika – Lista głównych rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie czynności oraz ochronę techniczną tajemnicy prawnie chronionej, w szczególności ochronę danych osobowych w nw. brzmieniu:

„Załącznik nr

Lista głównych rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie czynności oraz ochronę techniczną tajemnicy prawnie chronionej, w szczególności ochronę danych osobowych

1. ŚRODKI ORGANIZACYJNE:

1.1 Została opracowana i wdrożona polityka bezpieczeństwa;

1.2 Organizowane są cykliczne szkolenia dla pracowników/współpracowników z zasad bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych;

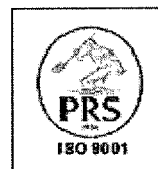
1.3 Realizowany jest zatwierdzony program podnoszenia świadomości z zakresu bezpieczeństwa informacji (szkolenia adaptacyjne, e-learning, pigułki wiedzy, szkolenia dedykowane, artykuły, symulowane ataki);

1.4 Oświadczenia do zachowania w poufności wszelkich informacji stanowiących tajemnicę przedsiębiorstwa są podpisywane przez pracowników/współpracowników przed rozpoczęciem pracy w organizacji;

1.5 Do przetwarzania informacji zostały dopuszczone wyłącznie uprawnione osoby;

1.6 Dane są klasyfikowane zgodnie z wytycznymi spółki. Klasyfikacja wspierana jest narzędziowo. Informację sklasyfikowane jako poufne podlegają dodatkowej ochronie wykorzystując mechanizmy szyfrujące;

1.7 Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;



1.8 Stosuje się politykę czystego biurka oraz czystego ekranu (blokowanie komputerów przy pustych stanowiskach, niepozostawianie dokumentacji na biurkach, zamykanie szafek z dokumentacją, itd.);

1.9 Realizowane są regularne audyty/kontrole bezpieczeństwa przetwarzania informacji;

1.10 Wdrożono skuteczny proces zgłaszania oraz obsługi zdarzeń/incydentów związanych z naruszeniem bezpieczeństwa informacji w tym naruszeniem ochrony danych osobowych;

1.11 Zdefiniowano i stosowana jest polityka kontroli dostęp do informacji. Przydzielanie uprawnień do informacji oraz ich modyfikacje realizowane są w oparciu o zasady minimalnych uprawnień i wiedzy koniecznej na podstawie udokumentowanych wniosków dostępowych;

1.12 Utworzono i uruchomiono jednostkę SOC (Security Operation Center) pracującą w trybie 24/7/365 w celu monitorowania infrastruktury i reagowania na incydenty cyberbezpieczeństwa;

1.13 Opracowano i wdrożono wewnętrzne standardy bezpieczeństwa wymagające stosowania zabezpieczeń adekwatnych do stopnia krytyczności i wrażliwości aktywów informacyjnych;

1.14 Zidentyfikowano krytyczne procesy i usługi oraz opracowano dla nich plany ciągłości działania oraz plany awaryjne w celu zapewnienia zdolności do szybkiego przywrócenia dostępności danych wrażliwych i dostępu do nich i usług krytycznych w razie incydentu fizycznego lub technicznego;

1.15 Wprowadzono do stosowania politykę prywatności.

1.16 Wprowadzono zasady bezpiecznej pracy zdalnej.

2. ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

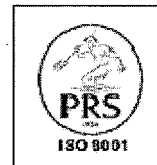
2.1 Stosowane są mechanizmy ochrony kont użytkowników identyfikujące podejrzane aktywności na ich kontach;

2.2 Logowanie do krytycznych usług realizowane jest z zastosowaniem dwuskładnikowego logowania;

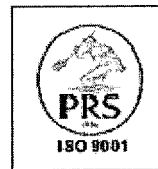
2.3 Dostęp do informacji oraz systemu operacyjnego komputera, w którym przetwarzane są informacje sklasyfikowane jako poufne (np. dane osobowe), zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Stosowana jest silna polityka haseł dostępowych;

2.4 Komputery, na których dochodzi do przetwarzania danych:

- pracują pod kontrolą aktualnego, wspieranego przez producenta systemu operacyjnego,
- posiadają uruchomioną systemową zaporę sieciową,
- posiadają aktualne systemy do ochrony przed złośliwym oprogramowaniem klasy EDR,
- posiadają zaszyfrowane dyski twarde, przy pomocy silnych protokołów szyfrujących,
- posiadają wygaszacze ekranów zabezpieczone hasłem.



- f. są centralnie nadzorowane i konfigurowane przez organizację (SOC+SIEM).
- 2.5 Stosowane są rozwiązania do automatyzacji konfiguracji i zabezpieczania stacji roboczych oraz mechanizmy identyfikujące stacje niezgodne z przyjętymi standardami bezpieczeństwa;
- 2.6 Urządzenia mobilne (smartfon, tablet), na których dochodzi do przetwarzania informacji:
- pracują pod kontrolą aktualnego, wspieranego przez producenta systemu operacyjnego,
 - posiadają zaszyfowaną pamięć urządzenia,
 - posiadają blokadę dostępu zabezpieczoną trudnym do odgadnięcia hasłem (litery i cyfry - najmniej 6 znaków), kodem PIN (minimum 6 cyfr), wzorem graficznym (minimum 6 znaków) lub zabezpieczeniem biometrycznym,
 - posiadają automatyczną blokadę dostępu do urządzenia po czasie nie dłuższym niż 1 minuta.
- 2.7 Dane sklasyfikowane jako poufne są w sposób automatyczny szyfrowane i ograniczone w dostępie z wykorzystaniem dedykowanego rozwiązania do klasyfikacji i ochrony informacji;
- 2.8 W uzasadnionych przypadkach stosowane są nośniki wymienne, które są szyfrowane (pendrive, CD/DVD, dysk zewnętrzny, itp.);
- 2.9 Informacje utrwalone w formie papierowej przechowywane są w zamknięciu;
- 2.10 Stosowany jest proces bezpiecznego niszczenia nośników informacji oparty na normie DIN 66399. Po ustaniu przydatności dokumentacja papierowa, magnetyczne dyski twarde oraz optyczne i elektroniczne nośniki danych podlegają procesowi bezpiecznego zniszczenia;
- 2.11 Zastosowano system rejestracji dostępu do systemu/bazy danych oraz użycia;
- 2.12 Stosowany jest system Web Application Firewall do ochrony krytycznych aktywów informacyjnych Spółki;
- 2.13 Zastosowano system Firewall do ochrony dostępu do sieci komputerowej;
- 2.14 Stosowane jest szyfrowanie komunikacji zewnętrznej oraz wewnętrznej przy pomocy silnych protokołów szyfrujących;
- 2.15 Identyfikowane są podatności systemów informatycznych. Ustalono proces zarządzania podatnościami technicznymi. Ustalono czasy remediacji podatności oraz ścieżki raportowania i eskalacji o przekroczeniach.
- 2.16 Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii informacji wrażliwych;
- 2.17 Zastosowano narzędzia klasy EDR (Endpoint Detection and Response – EDR) w celu wykrywania i reagowania na podejrzane aktywności urządzeń końcowych.
3. ŚRODKI OCHRONY FIZYCZNEJ DANYCH DLA OBIEKTÓW BIUROWYCH



- 3.1 Dostęp do pomieszczeń objęty jest systemem kontroli dostępu. Dostęp do stref Data Center mają tylko upoważnieni pracownicy, którzy świadczą bezpośrednio usługi utrzymania systemów w Data Center.
- 3.2 Pomieszczenia, w którym przetwarzane są informacje wyposażone są w system alarmowy przeciwwłamaniowy,
- 3.3 Dostęp do pomieszczeń, w których przetwarzane są informacje, kontrolowany jest przez system monitoringu z zastosowaniem kamer,
- 3.4 Dostęp do pomieszczeń, jest nadzorowany przez służbę ochrony. Funkcjonuje ochrona fizyczna obiektów Data Center w postaci koncesjonowanej służby ochrony. Uruchomiony jest elektroniczny monitoring wideo obiektów i stref bezpieczeństwa w obiektach, w trybie 24/365.
- 3.5 Zastosowano procedury zarządzania dostępem"

Odpowiedź: Zamawiający podtrzymuje zapisy § 15 ust. 3 PPU.

Zamawiający zawrze z Wykonawcą, z którym zostanie zawarta umowa podstawowa, stosowną umowę o przetwarzanie danych osobowych z uwzględnieniem uzgodnień pomiędzy stronami w zakresie końcowego brzmienia.

Pytanie nr 15

Wykonawca wobec konieczności uregulowania kwestii przetwarzania danych osobowych, wnosi o dodanie do § 15 PPU dodatkowego ustępu o nw. brzmieniu:

„Zamawiający oświadcza, że spełni w imieniu Wykonawcy – w zakresie udostępnionych danych osobowych - obowiązek informacyjny Wykonawcy, o którym mowa w art. 14 RODO – wobec osób i reprezentantów, którym Zamawiający posługuje się przy zawarciu Umowy, realizacji postanowień Umowy. Przedmiotowy obowiązek będzie wypełniany także względem każdej nowej osoby i reprezentanta, którego dane są lub mają być przekazane Wykonawcy. Obowiązek jest realizowany w oparciu o wzór klauzuli, stanowiącej Załącznik nr do Umowy”.

Wobec powyższego Wykonawca wnosi o dołączenie do umowy Załącznika – Klauzuli informacyjnej dla osób wskazanych do kontaktu w celu realizacji Umowy w nw. brzmieniu:

„Załącznik nr do Umowy

Klauzula informacyjna dla osób wskazanych do kontaktu w celu realizacji Umowy

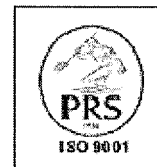
Administrator danych:

Administratorem Pani/Pana danych jest z siedzibą w (administrator).

Dane kontaktowe:

Z administratorem można się skontaktować poprzez e-mail: lub pisemnie na adres siedziby administratora.

Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.



Cele oraz podstawa prawna przetwarzania danych, prawnie uzasadnione interesy administratora:

Pani/Pana dane osobowe będą przetwarzane w celu wykonania umowy zawartej pomiędzy administratorem a a także – w zakresie prawnie usprawiedliwionego interesu administratora – w celu ustalenia, dochodzenia lub obrony przed roszczeniami z umowy, na podstawie odpowiednio art. 6 ust. 1 lit. c oraz art. 6 ust. 1 lit. f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Podstawą prawną przetwarzania danych jest niezbędność przetwarzania do realizacji prawnie uzasadnionego interesu administratora. Uzasadnionym interesem administratora jest możliwość wykonywania umów z kontrahentami oraz możliwość kontaktowania się w związku z wykonywaniem umowy.

Źródła i zakres danych pozyskiwanych od podmiotów trzecich:

Administrator pozyskał Pani/Pana dane osobowe: imię, nazwisko, stanowisko, nazwa i adres firmy, nr telefonu, adres e-mail od

Okres, przez który dane będą przetwarzane:

Pani/Pana dane osobowe będą przechowywane do momentu przedawnienia roszczeń z tytułu umowy zawartej pomiędzy administratorem a

Odbiorcy danych:

Pani/Pana dane mogą:

- organom państwowym lub innym podmiotom uprawnionym na podstawie przepisów prawa,
- osobom upoważnionym przez administratora,
- podmiotom przetwarzającym dane osobowe na zlecenie administratora celem wykonania ciążących na administratorze obowiązków, m.in.:
 - podwykonawcom,
 - podmiotom prowadzącym działalność pocztową lub kurierską,
- podmiotom wspierającym administratora w prowadzonej działalności na jego zlecenie, w szczególności dostawcom zewnętrznych systemów wspierającym działalność administratora,
 - przy czym takie podmioty przetwarzają dane na podstawie umowy z administratorem i wyłącznie zgodnie z poleceniami administratora.

Przekazywanie danych osobowych poza EOG:

Dane osobowe będą przechowywane na serwerach zlokalizowanych w Unii Europejskiej i mogą być przekazane - na podstawie standardowych klauzul ochrony danych - do państwa trzeciego w związku z korzystaniem przez administratora z rozwiązań chmurowych dostarczanych przez firmę Microsoft. Stosowane przez Microsoft standardowe klauzule umowne zgodne z wzorcami zatwierdzonymi przez Komisję Europejską, dostępne są pod adresem: <https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx> w części Product Terms.

Prawa osoby, której dane dotyczą:

Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania, ich usunięcia lub ograniczenia ich przetwarzania.



Wojewódzki Szpital Zespolony w Kielcach

25-736 Kielce, ul. Grunwaldzka 45

tel: 41/36-71-301, fax: 41/34-50-623

e-mail: szpital@wszkielce.pl

www.wszkielce.pl



W zakresie, w jakim podstawą przetwarzania Pani/Pana danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, przysługuje Pani/Panu prawo wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych osobowych.

W celu skorzystania z powyższych praw należy skontaktować się z administratorem danych lub z inspektorem ochrony danych.

Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

Profilowanie

Informujemy, że nie podejmujemy decyzji w sposób zautomatyzowany i Pani/Pana dane nie są profilowane”

Odpowiedź: Zamawiający podtrzymuje zapisy § 15 ust. 3 PPU

Zamawiający zawrze z Wykonawcą, z którym zostanie zawarta umowa podstawowa, stosowną umowę o przetwarzanie danych osobowych z uwzględnieniem uzgodnień pomiędzy stronami w zakresie końcowego brzmienia.

Przesunięcie terminu składania i otwarcia ofert wraz z terminem związania ofertą

Zamawiający Wojewódzki Szpital Zespolony w Kielcach, działając na podstawie art. 284 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2024 r. poz. 1320 ze zm.), przesuwa termin składania i otwarcia ofert wraz z terminem związania ofertą:

NOWE TERMINY:

Termin składania ofert: 13.08.2025 r. godz. 09:00

Termin otwarcia ofert: 13.08.2025 r. godz. 09:30

Termin związania ofertą: 14.09.2025 r

Wprowadzone modyfikacje i wyjaśnienia treści Specyfikacji są wiążące i należy je uwzględnić w treści składanej oferty.

W załączniku zmodyfikowane Załączniki nr 2 i 3 do SWZ

DZIAŁ ZAMÓWIEŃ PUBLICZNYCH

Renata Łastowska
Inspektor
Łastowska

KIEROWNIK

Działu Zamówień Publicznych
2025-08-05
mgr Sebastian Szaniawski

2025-08-07
DYREKTOR
Wojewódzkiego Szpitala Zespolonego w Kielcach

Marcin Martyniak

mgr Jolanta Wróblewska-Więcek
RADCA PRAWNY
KL-1220

Dział Zamówień Publicznych

tel: 41/36-71-269

renata.lastowska@wszkielce.pl