



Pomorski Uniwersytet Medyczny w Szczecinie

## SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

ZAPRASZA DO ZŁOŻENIA OFERTY W POSTĘPOWANIU  
O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO  
PROWADZONYM W TRYBIE PRZETARGU NIEOGRANICZONEGO O NAZWIE:

***System ochrony poczty elektronicznej pracowników PUM***

**SYGNATURA POSTĘPOWANIA: DZP-262-7/2019**

Szczecin, dnia 18.02.2019 r.

KANCLERZ  
Pomorskiego Uniwersytetu Medycznego  
w Szczecinie  
*mgr inż. Krzysztof Goralski*

.....

*Zatwierdzam*

## **SPIS TREŚCI :**

<b>Rozdział I</b>	Nazwa i dane kontaktowe do zamawiającego, sposób porozumiewania się z zamawiającym, podstawa prawna, dane dotyczące ogłoszenia umieszczonego w DUUE, podpis elektroniczny, ochrona danych osobowych
<b>Rozdział II</b>	Słownik CPV, wybór procedury
<b>Rozdział III</b>	Oferty i dokumenty/oświadczenia składane wraz z ofertą, opis sposobu przygotowania oferty
<b>Rozdział IV</b>	Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych i katalog informacji przekazywanych przy ich użyciu
<b>Rozdział V</b>	Wycofanie oferty, oferta po terminie, związanie ofertą, jawność postępowania i tajemnica przedsiębiorstwa
<b>Rozdział VI</b>	Termin złożenia ofert, otwarcie ofert, informacja z otwarcia ofert, oświadczenie o grupie kapitałowej
<b>Rozdział VII</b>	Podwykonawcy i podmioty trzecie
<b>Rozdział VIII</b>	Oferty wspólne
<b>Rozdział IX</b>	Warunki udziału w postępowaniu, dokumenty i oświadczenia żądane przez Zamawiającego, sposób wypełnienia JEDZa, wezwanie do uzupełnienia
<b>Rozdział X</b>	Wadium i sposób jego wniesienia
<b>Rozdział XI</b>	Kryteria oceny ofert i opis sposobu oceny ofert
<b>Rozdział XII</b>	Opis sposobu obliczania ceny oraz rozliczenia z wykonawcą
<b>Rozdział XIII</b>	Postępowanie po otwarciu ofert, ocena ofert i wybór najkorzystniejszej oferty
<b>Rozdział XIV</b>	Termin wykonania zamówienia, okres gwarancji i rękojmi
<b>Rozdział XV</b>	Zawarcie umowy o zamówienie publiczne
<b>Rozdział XVI</b>	Środki ochrony prawnej
<b>Rozdział XVII</b>	Opis przedmiotu zamówienia

## **Załączniki:**

1. Wzór umowy
2. Regulamin platformazakupowa.pl

## **Dodatkowo do wykorzystania przez wykonawców:**

Wzór formularza ofertowego;

Jednolity Europejski Dokument Zamówienia;

Wzór oświadczenia o przynależności/braku przynależności do grupy kapitałowej;

Wzór zobowiązania podmiotu trzeciego.

## ROZDZIAŁ I. Nazwa i dane kontaktowe do zamawiającego, sposób porozumiewania się z zamawiającym, podstawa prawna, dane dotyczące ogłoszenia umieszczonego w DUUE, podpis elektroniczny, ochrona danych osobowych

### Zamawiający:

Pomorski Uniwersytet Medyczny w Szczecinie

ul. Rybacka 1, 70-204 Szczecin

NIP 852-000-67-57

REGON 000288886

strona internetowa, na której zamieszczone są ogłoszenie, dokumenty i informacje dotyczące przedmiotowego postępowania: <https://bip.pum.edu.pl/artykuly/215/uslugi>

Platforma zakupowa: [www.platformazakupowa.pl](http://www.platformazakupowa.pl)

telefony przetargi: (91) 48-00-778

(91) 48-00-779

e-mail przetargi: [przetargi@pum.edu.pl](mailto:przetargi@pum.edu.pl)

Wykonawca ma możliwość przysłać e-mail lub wiadomość za pośrednictwem platformy zakupowej przez całą dobę.

godziny urzędowania zamawiającego: od poniedziałku do piątku 7:30 do 15:30

Podstawa prawna: Ustawa z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2018 r.; poz. 1986 t.j.), zwana dalej „ustawą pzp”.

Rozporządzenie Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126), ze zmianą Rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 16 października 2018 r. zmieniające rozporządzenie w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz.U. z 2018 r., poz. 1993), zwane dalej „**rozporządzeniem o dokumentach**”.

Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych (Dz.U. z 2017 r., poz. 1320) ze zmianą Rozporządzenie Prezesa Rady Ministrów z dnia 17 października 2018 r. zmieniające rozporządzenie w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych (Dz.U. z 2018 r., poz. 1991), zwane dalej „**rozporządzeniem o środkach komunikacji elektronicznej**”

Jednolity Europejski Dokument Zamówienia, zwany dalej „**JEDZ**”

Ogłoszenie o zamówieniu zostało przekazane Urzędowi Publikacji Unii Europejskiej w dniu 18.02.2019 r.

1. Komunikacja pomiędzy zamawiającym, a wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej (e-mail lub przy użyciu formularzy na [www.platformazakupowa.pl](http://www.platformazakupowa.pl)).
2. Wszelkie informacje, wezwania, powiadomienia, wnioski o wyjaśnienie treści siwz, inne wnioski, odpowiedzi na pytania, wyjaśnienia, itd. zamawiający i wykonawcy będą przekazywać wyłącznie przy użyciu środków komunikacji elektronicznej.
3. Wszystkie dokumenty i oświadczenia **nie wymagające szyfrowania**, czyli dokumenty i oświadczenia składane po otwarciu ofert, mogą być składane przy użyciu formularzy dostępnych na platformie zakupowej [www.patformazakupowa.pl](http://www.patformazakupowa.pl) albo za pośrednictwem poczty elektronicznej na adres [przetargi@pum.edu.pl](mailto:przetargi@pum.edu.pl), poprzez „Wyślij wiadomość” lub z dodaniem załączników.
4. Oferta oraz dokumenty i oświadczenia (JEDZ, pełnomocnictwa, zobowiązanie podmiotów trzecich), składane wraz z ofertą, **wymagają szyfrowania** i mogą zostać złożone wyłącznie za pośrednictwem platformy zakupowej na [www.platformazakupowa.pl](http://www.platformazakupowa.pl). **Nie jest możliwe** przesłanie oferty, a także oświadczeń JEDZ, zobowiązań podmiotów trzecich, pełnomocnictw i innych oświadczeń lub dokumentów dołączanych do oferty i wysyłanych do upływu terminu składania ofert, za pośrednictwem poczty elektronicznej, gdyż taki sposób użycia środka komunikacji elektronicznej nie zapewnia szyfrowania.
5. Komunikacja poprzez [www.patformazakupowa.pl](http://www.patformazakupowa.pl), za pomocą przycisku „Wyślij wiadomość”, umożliwia dodanie do treści wysyłanej wiadomości plików lub spakowanego katalogu (załączników). Występuje limit objętość plików lub spakowanego katalogu w zakresie całej wiadomości do 1 GB przy maksymalnej ilości 20 plików lub spakowanych katalogów.
6. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń, składane są przez wykonawcę poprzez [www.patformazakupowa.pl](http://www.patformazakupowa.pl) za pomocą przycisku „Wyślij wiadomość” lub za pośrednictwem poczty elektronicznej na adres [przetargi@pum.edu.pl](mailto:przetargi@pum.edu.pl) jako załączniki. Oświadczenia, informacje, wnioski od wykonawców, nie wymagające postaci elektronicznej (np. wnioski o wyjaśnienie treści siwz, prośby o przekazanie protokołu postępowania, oświadczenie o przedłużeniu terminu składania ofert), mogą być złożone do zamawiającego w treści wiadomości e-mail.
7. Kwalifikowany podpis elektroniczny niezbędny jest do podpisania oferty, oświadczeń JEDZ, dokumentów i oświadczeń wymienionych w rozporządzeniu o dokumentach, poświadczania dokumentów i oświadczeń za zgodność z oryginałem oraz do podpisywania pełnomocnictw.
8. Oświadczenia woli, składane przez zamawiającego i wykonawcę uważa się za złożone z chwilą, gdy doszły do adresata w taki sposób, że mógł on zapoznać się z jego treścią. Odwołanie takiego oświadczenia jest skuteczne, jeżeli doszło z tym oświadczeniem lub wcześniej.

9. Datą wpłynięcia oświadczenia lub informacji do zamawiającego lub wykonawcy jest data i godzina jego faktycznego dotarcia do adresata, w taki sposób, że mógł on się zapoznać z jego treścią. Nie zapoznanie się adresata z treścią oświadczenia lub informacji, z uwagi na ustalone godziny urzędowania zamawiającego lub wykonawcy nie wstrzymuje biegu terminów.
10. Osobami uprawnionymi do kontaktowania się z wykonawcami są pracownicy Działu Zamówień Publicznych: p. Marzena Kopacka, p. Izabela Leżańska oraz Kierownik Działu Informatyki p. Krzysztof Kozakowski.
11. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:
  - a) administratorem Pani/Pana danych osobowych jest **Pomorski Uniwersytet Medyczny w Szczecinie, ul. Rybacka 1, 70-204 Szczecin**;
  - b) kontakt z Inspektorem Ochrony Danych Pomorskiego Uniwersytetu Medycznego w Szczecinie możliwy jest pod numerem tel. 91 48 00 790 lub adresem e-mail: [iod@pum.edu.pl](mailto:iod@pum.edu.pl);
  - c) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu, związanym z postępowaniem o udzielenie zamówienia pn.: **„System ochrony poczty elektronicznej pracowników PUM”**, prowadzonym w trybie przetargu nieograniczonego, nr postępowania DZP-262-7/2019;
  - d) w przypadku wyboru oferty najkorzystniejszej Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z realizacją umowy na system ochrony poczty elektronicznej pracowników PUM;
  - e) odbiorcami Pani/Pana danych osobowych będą:
    - osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania, w oparciu o art. 8 oraz art. 96 ust. 3 ustawy pzp,
    - upoważnieni pracownicy Administratora oraz podmioty świadczące dla Administratora usługi w szczególności informatyczne, marketingowe, prawne, windykacyjne, transportowe, kurierskie, pocztowe, niszczenia dokumentów, niszczenia dokumentów, banki i instytucje płatnicze,
    - współpracownicy kancelarii prawnych i osoby współpracujące z zamawiającym,
    - instytucje upoważnione na mocy prawa zgodnie z ich kompetencjami i uprawnieniami,
    - w przypadku realizacji umowy – pracownicy zamawiającego oraz inne podmioty zatrudnione przez zamawiającego do nadzoru nad realizacją umowy;



- f) Pani/Pana dane osobowe przechowywane będą przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, (obejmującym w szczególności okres gwarancji i rękojmi, objętych realizacją umowy), chyba że niezbędny będzie dłuższy okres przetwarzania, np.: z uwagi na obowiązki archiwizacyjne, dochodzenie roszczeń itp.;
- g) obowiązek podania przez Pana/Panią danych osobowych bezpośrednio Pana/Panią dotyczących jest wymogiem ustawowym, określonym w przepisach ustawy pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, konsekwencje niepodania określonych danych wynikają z ustawy pzp;
- h) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- i) posiada Pani/Pan:
- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą pzp oraz nie może naruszać integralności protokołu oraz jego załączników*);
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*);
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- j) nie przysługuje Pani/Panu:
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. b i c RODO.

## ROZDZIAŁ II. Słownik CPV, wybór procedury

1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy PZP.
2. Szacunkowa wartość przedmiotowego zamówienia jest mniejsza niż kwoty, określone w przepisach, wydanych na podstawie art. 11 ust. 8 ustawy PZP, jednakże z uwagi na to, że postępowanie jest częścią zamówienia o wartości przewyższającej kwoty, określone w przepisach, wydanych na podstawie art. 11 ust. 8 ustawy PZP, postępowanie jest prowadzone zgodnie z przepisami, właściwymi dla wartości łącznej.
3. Niniejsza specyfikacja podlega udostępnieniu w formie pliku do pobrania na stronie internetowej Zamawiającego: <https://bip.pum.edu.pl/artykuly/215/uslugi>, od dnia opublikowania ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej.
4. Zamówienie jest realizowane w ramach projektu „Progressio – Zintegrowany Rozwój Pomorskiego Uniwersytetu Medycznego w Szczecinie”, współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020.
5. Przedmiotem postępowania (zamówienia) jest:  
**System ochrony poczty elektronicznej pracowników PUM**
6. Wspólnotowy Słownik Zamówień CPV: 48223000-7 Pakiety oprogramowania do poczty elektronicznej.
7. Niniejsze postępowanie prowadzone jest zgodnie z art. 24aa ustawy pzp. Zgodnie ze wskazaną procedurą zamawiający dokona oceny ofert, a następnie zbada, czy wykonawca, którego oferta została najwyżej oceniona nie podlega wykluczeniu z postępowania. Jeśli wykonawca wybrany uchyli się od podpisania umowy lub nie wniesie zabezpieczenia należytego wykonania umowy zamawiający zbada, czy nie podlega wykluczeniu wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.
8. Kod NUTS - PL424 Miasto Szczecin.

## ROZDZIAŁ III. Oferty i dokumenty/oświadczenia składane wraz z ofertą, opis sposobu przygotowania oferty

1. **Oferta**, składana w niniejszym postępowaniu jest zobowiązaniem wykonawcy do zgodnego z oczekiwaniami zamawiającego, wyrażonymi w siwz, na warunkach wskazanych przez zamawiającego, wykonania zamówienia, za określoną w formularzu ofertowym cenę.
2. Na ofertę składają się: oświadczenie wykonawcy co do spełnienia na rzecz zamawiającego określonego w niniejszej siwz świadczenia, w zadeklarowany sposób i za oferowaną cenę, oraz wszystkie pozostałe wymagane dokumenty i oświadczenia w tym JEDZ.
3. Wykonawcy sporządzają oferty zgodnie z wymaganiami siwz.

4. Zamawiający przekazuje **wzór formularza ofertowego** do wykorzystania przez wykonawców. Wykonawcy mogą go nie wykorzystać i sporządzić ofertę na własnym formularzu, pod warunkiem, że jego treść odpowiadać będzie warunkom określonym przez zamawiającego w siwz oraz warunkom określonym w ustawie pzp.
5. Oferty i oświadczenia muszą być sporządzone w języku polskim. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski.
6. Wraz z ofertą wykonawca jest zobowiązany złożyć:
  - a) **JEDZ** stanowiący **wstępne oświadczenie, że wykonawca nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu;**
  - b) **JEDZe podmiotów**, na zasoby których powołuje się wykonawca, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu,
  - c) zobowiązanie podmiotów trzecich, jeśli wykonawca będzie polegał na ich potencjale,
  - d) wadium wnoszone w formie niepieniężnej.
7. **Ofertę oraz JEDZ, a także wszelkie inne oświadczenia i dokumenty, składane wraz z ofertą sporządza się, pod rygorem nieważności, w formie elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.** JEDZe podmiotów innych niż wykonawca, sporządzone w formie elektronicznej, muszą być opatrzone kwalifikowanymi podpisami elektronicznymi przez podmioty, których one dotyczą.
8. Oferta powinna być sporządzona w postaci elektronicznej i opatrzona kwalifikowanym podpisem elektronicznym przez osoby upoważnione do składania oświadczeń woli w imieniu wykonawcy. Pełnomocnictwo do podpisania oferty musi być sporządzone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym i być dołączone do oferty w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza, o ile nie wynika ono z innych dokumentów załączonych przez wykonawcę.
9. Zaleca się by w formularzu ofertowym wykonawcy wpisali dane teleadresowe, na które ma być kierowana korespondencja od zamawiającego i osoby do bieżącego kontaktu z zamawiającym.
10. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
11. Wykonawca składa tylko jedną ofertę.
12. Zamawiający nie dopuszcza składania ofert wariantowych.
13. Zamawiający nie przewiduje udzielania zamówień podobnych, na podstawie art. 67 ust. 1 pkt 6) ustawy pzp.
14. W przedmiotowym postępowaniu nie zostanie przeprowadzona aukcja elektroniczna.
15. Zamawiający nie przewiduje zawarcia umowy ramowej.

#### **ROZDZIAŁ IV. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych i katalog informacji przekazywanych przy ich użyciu**

1. Ofertę, JEDZ, pełnomocnictwa, oświadczenia i dokumenty, składane wraz z ofertą można złożyć wyłącznie za pośrednictwem platformy [www.platformazakupowa.pl](http://www.platformazakupowa.pl).
2. Wykonawca składa ofertę za pośrednictwem **Formularza składania oferty** dostępnego na [www.platformazakupowa.pl](http://www.platformazakupowa.pl).



3. Wymagania techniczne i organizacyjne, dotyczące ofert opisane zostały w Regulaminie platformazakupowa.pl, który stanowi załącznik nr 2 do niniejszej siwz, a także dostępny jest na <https://platformazakupowa.pl/strona/1-regulamin>. Przed złożeniem oferty wykonawca zobowiązany jest do zapoznania się z treścią regulaminu.
4. Minimalne wymagania techniczne umożliwiające korzystanie ze Strony [platformazakupowa.pl](https://platformazakupowa.pl) to przeglądarka internetowa Internet Explorer, Chrome i FireFox w najnowszej dostępnej wersji, z włączoną obsługą języka Javascript, akceptująca pliki typu „cookies” oraz łącze internetowe o przepustowości, co najmniej 256 kbit/s; [platformazakupowa.pl](https://platformazakupowa.pl) jest zoptymalizowana dla minimalnej rozdzielczości ekranu 1024x768 pikseli.
5. Występuje limit objętości plików lub spakowanych folderów w zakresie całej oferty do **1 GB** przy maksymalnej ilości **20 plików lub spakowanych folderów**.
6. W przypadku większych plików zaleca się skorzystać z instrukcji pakowania plików dzieląc je na mniejsze paczki, po np. 75 MB każda.
7. Instrukcja pakowania plików i inne instrukcje są dostępne pod adresem internetowym: <https://platformazakupowa.pl/strona/45-instrukcje>.
8. Przy dużych plikach kluczowe jest łącze internetowe i dostępna przepustowość łącza oraz zaplanowanie złożenia oferty z odpowiednim wyprzedzeniem, aby zdążyć w terminie złożenia oferty.
9. Za datę przekazania oferty i dokumentów/oświadczeń składanych wraz z ofertą przyjmuje się datę ich przekazania w systemie wraz z wgraniem paczki w formacie XML w drugim kroku składania oferty, poprzez kliknięcie przycisku „**Złóż ofertę**” i wyświetlaniu komunikatu, że oferta została złożona.
10. Do oferty należy dołączyć wszystkie wymagane w ogłoszeniu, i siwz dokumenty - w tym także JEDZ, ewentualne pełnomocnictwa, zobowiązanie podmiotu trzeciego, w postaci elektronicznej.
11. Po wypełnieniu **Formularza składania oferty** i załadowaniu wszystkich wymaganych załączników należy kliknąć przycisk „**Przejdź do podsumowania**”.
12. Oferta i dokumenty/oświadczenia składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem. Taki podpis na platformie zakupowej wykonawca może złożyć:
  - bezpośrednio na dokumencie przesłanym do systemu lub/i
  - dla całego pakietu dokumentów w kroku 2 **Formularza składania oferty** (po kliknięciu w przycisk „**Przejdź do podsumowania**”).
13. Ścieżka dla złożenia podpisu kwalifikowanego **na każdym dokumencie osobno**:
  - Wykonawca musi podpisać plik, który zamierza dołączyć do oferty kwalifikowanym podpisem elektronicznym,
  - Następnie w drugim kroku składania oferty należy:
    - sprawdzić poprawność złożonej oferty oraz załączonych plików,
    - pobrać plik w formacie XML,
    - po wgraniu XML bez podpisu system dokona wstępnej analizy i wyświetli informację o błędzie,
    - informację o tym, czy plik XML został podpisany prawidłowo lub nie należy traktować jako weryfikację pomocniczą, gdyż to zamawiający przeprowadzi proces badania ofert w postępowaniu,



- pliku XLM nie należy modyfikować ani zmieniać, gdyż służy on do celów dowodowych,
  - Przyczyny błędnej walidacji podpisu mogą być następujące:
    - ✓ brak podpisu na dokumencie XML,
    - ✓ podpis kwalifikowany utracił ważność,
    - ✓ niewłaściwy formatu podpisu,
    - ✓ użycie podpisu niekwalifikowanego,
    - ✓ zmodyfikowano plik XML,
    - ✓ załączenie przez wykonawcę niewłaściwego pliku XML.
  - niezależnie od wyświetlonego komunikatu wykonawca może kliknąć przycisk „Złóż ofertę”, aby zakończyć etap składania oferty, musi się jednak upewnić, czy błąd nie jest spowodowany błędami o których mowa wyżej,
  - następnie system zaszyfruje ofertę wykonawcy, tak by ta była niedostępna dla zamawiającego do terminu otwarcia ofert,
  - ostatnim krokiem jest wyświetlenie się komunikatu i przesłanie wiadomości email z [www.platformazakupowa.pl](http://www.platformazakupowa.pl) z informacją na temat złożonej oferty (Uwaga ! W przypadku składania kolejnej oferty i wycofania poprzedniej, jeżeli użytkownik nie jest zalogowany, to do jego identyfikacji potrzebne jest kliknięcie w mail potwierdzający wycofanie złożonej oferty. W link ten należy kliknąć do czasu przewidzianego na składanie ofert. Kliknięcie linku po terminie sprawi, że straci on ważność),
  - w celach odwoławczych z uwagi na zaszyfrowanie oferty na [www.platformazakupowa.pl](http://www.platformazakupowa.pl) wykonawca powinien przechowywać kopię swojej oferty wraz z pobranym plikiem XML na swoim komputerze.
14. Ścieżka dla złożenia podpisu kwalifikowanego na całej paczce XML:
- Należy dołączyć w kroku pierwszym pliki do oferty,
  - Następnie w drugim kroku składania oferty należy:
    - sprawdzić poprawność złożonej oferty oraz załączonych plików,
    - pobrać plik w formacie XML,
    - wykonawca wgrywa plik zawierający podpis pobranej oferty XML opatrzony kwalifikowanym podpisem lub kwalifikowanymi podpisami w formacie XADES (XAdES),
    - jeżeli plik XML został opatrzony kwalifikowanym podpisem elektronicznym i podpis ten jest ważny wyświetli się komunikat potwierdzający prawidłowości podpisu wraz z informacją o osobie podpisującej,
    - gdy plik nie został opatrzony kwalifikowanym podpisem elektronicznym to w takiej sytuacji system wyświetli informację o błędzie (braku podpisu, braku ważnego podpisu lub modyfikacja pobranego pliku XML),
    - informację o tym, czy plik XML został podpisany prawidłowo lub nie należy traktować jako weryfikację pomocniczą, gdyż to zamawiający przeprowadzi proces badania ofert w postępowaniu,
    - pliku XLM nie należy modyfikować ani zmieniać, gdyż służy on do celów dowodowych,
    - przyczyny błędnej walidacji podpisu mogą być następujące:
      - ✓ brak podpisu na dokumencie XML,
      - ✓ podpis kwalifikowany utracił ważność,



- ✓ niewłaściwy formatu podpisu,
- ✓ użycie podpisu niekwalifikowanego,
- ✓ zmodyfikowano plik XML,
- ✓ załączenie przez wykonawcę niewłaściwego pliku XML,
- niezależnie od wyświetlonego komunikatu wykonawca może kliknąć przycisk „Złóż ofertę”, aby zakończyć etap składania oferty, musi się jednak upewnić, czy błąd nie jest spowodowany błędami o których mowa wyżej,
- następnie system zaszyfruje ofertę wykonawcy, tak by ta była niedostępna dla zamawiającego do terminu otwarcia ofert,
- ostatnim krokiem jest wyświetlenie się komunikatu i przesłanie wiadomości e-mail z [www.platformazakupowa.pl](http://www.platformazakupowa.pl) z informacją na temat złożonej oferty (Uwaga! W przypadku składania kolejnej oferty i wycofania poprzedniej, jeżeli użytkownik nie jest zalogowany, to do jego identyfikacji potrzebne jest kliknięcie w mail potwierdzający wycofanie złożonej oferty. W link ten należy kliknąć do czasu przewidzianego na składanie ofert. Kliknięcie linku po terminie sprawi, że straci on ważność),
- w celach odwoławczych z uwagi na zaszyfrowanie oferty na [www.platformazakupowa.pl](http://www.platformazakupowa.pl) wykonawca powinien przechowywać kopię swojej oferty wraz z pobranym i podpisanym plikiem XML na swoim komputerze.

## ROZDZIAŁ V. Wycofanie oferty, oferta po terminie, związanie ofertą, jawność postępowania i tajemnica przedsiębiorstwa

1. Wykonawca może przed upływem terminu do składania ofert wycofać ofertę za pośrednictwem **Formularza składania oferty**.
2. Z uwagi na to, że oferta wykonawcy jest zaszyfrowana, nie można jej edytować. Przez zmianę oferty rozumie się złożenie nowej oferty i wycofanie poprzedniej, jednak należy to zrobić przed upływem terminu składania ofert w postępowaniu.
3. Złożenie nowej oferty powoduje wycofanie oferty poprzednio złożonej.
4. Jeśli wykonawca składający ofertę jest zautoryzowany (**zalogowany**), to wycofanie oferty następuje od razu po złożeniu nowej oferty.
5. Jeżeli oferta składana jest przez niezautoryzowanego wykonawcę, (niezalogowany lub nieposiadający konta), to wycofanie oferty musi być przez niego potwierdzone:
  - przez kliknięcie w link wysłany w wiadomości email, który musi być zgodny z adresem e-mail, podanym podczas pierwotnego składania oferty lub
  - zalogowanie i kliknięcie w przycisk **Potwierdź ofertę**.
6. Potwierdzeniem wycofania oferty w przypadku ust. 5 tირet pierwszy jest data kliknięcia w przycisk **Wycofaj ofertę** i potwierdzenie tej akcji.
7. Wycofanie oferty możliwe jest do zakończeniu terminu składania ofert w postępowaniu.
8. Wycofanie złożonej oferty powoduje, że zamawiający nie będzie miał możliwości zapoznania się z nią po upływie terminu składania ofert.
9. Wykonawca po upływie terminu składania ofert nie może dokonać zmiany złożonej oferty.

10. Złożenie oferty po terminie składania ofert jest możliwe tylko poprzez kliknięcie przycisku „**Odblokuj formularz**”. Po złożeniu takiej oferty wykonawca otrzymuje automatyczny komunikat dotyczący tego, że oferta została złożona po terminie.
11. W przypadku złożenia oferty po terminie Zamawiający niezwłocznie zawiadomi Wykonawcę o jej złożeniu po terminie oraz zwróci ją po upływie terminu do wniesienia odwołania.
12. Postępowanie o udzielenie przedmiotowego zamówienia jest jawne.
13. Oferty są jawne od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane, oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
14. Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.
15. Wykonawca nie może zastrzec swojej nazwy (firmy) oraz adresu, a także informacji dotyczących ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
16. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać załączone w osobnym miejscu w kroku 1 składania oferty, przeznaczonym na zamieszczenie tajemnicy przedsiębiorstwa. Zaleca się, aby każdy dokument zawierający tajemnicę przedsiębiorstwa został zamieszczony w odrębnym pliku.
17. Wykonawca pozostaje związany ofertą przez okres 60 dni, tj. do dnia 24 maja 2019 r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
18. Jeżeli wykonawca zdecyduje o przedłużeniu ważności oferty, oświadczenie woli w sprawie przedłużenia terminu związania ofertą musi zostać złożone zamawiającemu przed upływem terminu związania ofertą.

## ROZDZIAŁ VI. Termin złożenia ofert, otwarcie ofert, informacja z otwarcia ofert, oświadczenie o grupie kapitałowej

1. Oferty w formie elektronicznej należy złożyć do dnia **26 marca 2019 r. do godz. 12:00**.
2. Otwarcie ofert nastąpi w siedzibie zamawiającego w dniu **26 marca 2019 r. o godz. 12:30 w pokoju 215**. Zamawiający zastrzega sobie możliwość zmiany pomieszczenia, w którym nastąpi otwarcie ofert w przypadku braku dostępności wskazanego pomieszczenia. Wszyscy zainteresowani, którzy stawią się w oznaczonym w SIWZ terminie i miejscu zostaną w takiej sytuacji poproszeni o przejście do innego pomieszczenia znajdującego się w siedzibie Zamawiającego.

3. Zamawiający bezpośrednio przed otwarciem ofert poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. System [www.platformazakupowa.pl](http://www.platformazakupowa.pl) będzie automatycznie numerował oferty. Po upływie terminu wyznaczonego na otwarcie ofert zostaną one automatycznie odszyfrowane. Otwarcie ofert nastąpi w kolejności, w jakiej zostały one złożone.
5. Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie internetowej informacje dotyczące: kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia, firm oraz adresów wykonawców, którzy złożyli oferty w terminie, cen, okresu gwarancji i rękojmi, terminu wykonania zamówienia i warunków płatności zawartych w ofertach.
6. Wykonawca, bez wezwania ze strony zamawiającego, **w terminie 3 dni** od dnia zamieszczenia przez zamawiającego na stronie internetowej informacji z otwarcia ofert złoży **oświadczenie o przynależności/braku przynależności do grupy kapitałowej**. Jeśli wykonawca przynależy do grupy kapitałowej wspólnie z innym wykonawcą, który złożył ofertę w postępowaniu, wraz ze złożeniem oświadczenia może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. W przypadku ofert wspólnych oświadczenie o przynależności/braku przynależności do grupy kapitałowej i ewentualne dowody na brak zakłócenia konkurencji składa każdy z wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
7. Oświadczenie o przynależności/braku przynależności do grupy kapitałowej musi zostać złożone **w formie elektronicznej i podpisane kwalifikowanym podpisem elektronicznym**. Oświadczenie to może zostać do zamawiającego przesłane w formie załącznika elektronicznego za pośrednictwem platformy [www.platformazakupowa.pl](http://www.platformazakupowa.pl), lub za pośrednictwem e-maila [przetargi@pum.edu.pl](mailto:przetargi@pum.edu.pl).
8. Zamawiający przekazuje wzór oświadczenia o przynależności/braku przynależności do grupy kapitałowej do wykorzystania przez wykonawców. Wykonawcy mogą go nie wykorzystać i sporządzić oświadczenie na własnym formularzu, pod warunkiem, że ich treść odpowiadać będzie warunkom określonym przez zamawiającego w siwz oraz warunkom określonym w ustawie PZP.

## ROZDZIAŁ VII. Podwykonawcy i podmioty trzecie

1. Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie wykonawca zamierza powierzyć podwykonawcom i podania firm wykonawców.
2. Zamawiający nie żąda złożenia przez wykonawców JEDZów podwykonawców.
3. Podmiotem trzecim w niniejszym zamówieniu jest każdy podmiot, na zdolnościach zawodowych którego polega Wykonawca, w celu spełnienia warunków udziału w postępowaniu.
4. Wykonawca może w celu potwierdzenia spełnienia warunków udziału w postępowaniu, polegać na zdolnościach zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia warunków udziału w

postępowaniu, w zakresie, w jakim powołuje się na ich zasoby, składa wraz z ofertą **JEDZ dotyczący każdego z tych podmiotów.**

6. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając **zobowiązanie tych podmiotów** do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. Zobowiązanie podmiotów trzecich musi być złożone już wraz z ofertą Wykonawcy.
7. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności zawodowe, pozwalają na wykazanie przez Wykonawcę spełnienia warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia.
8. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda informacji zawierającej dane dotyczące: zakresu dostępnych Wykonawcy zasobów innego podmiotu, sposobu wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego, zakresu i okresu udziału innego podmiotu przy wykonywaniu zamówienia publicznego.
9. Jeżeli zdolności zawodowe podmiotu, na zdolnościach którego polega Wykonawca nie potwierdzą spełnienia przez Wykonawcę warunków udziału w postępowaniu lub wobec tego podmiotu zachodzą podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w określonym terminie zastąpił ten podmiot innym podmiotem lub podmiotami lub zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności zawodowe, wymagane przez Zamawiającego.
10. Zamawiający przekazuje wzór zobowiązania podmiotu trzeciego do wykorzystania przez wykonawców. Wykonawcy mogą go nie wykorzystać i sporządzić zobowiązanie na własnym formularzu, pod warunkiem, że jego treść odpowiadać będzie warunkom określonym przez zamawiającego w siwz oraz warunkom określonym w ustawie PZP.

## ROZDZIAŁ VIII. Oferty wspólne

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
2. Wykonawcy składający ofertę wspólną ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Upoważnienie do złożenia oferty albo do złożenia oferty i podpisania umowy w sprawie zamówienia publicznego powinno jasno wynikać z treści pełnomocnictwa.
3. Do oferty wspólnej Wykonawcy dołączają pełnomocnictwo, w postaci elektronicznej, opatrzone podpisem elektronicznym w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza.

4. Zaleca się by w formularzu ofertowym Wykonawcy składający ofertę wspólną wpisali dane teleadresowe, na które ma być kierowana korespondencja od Zamawiającego (do którego z podmiotów) i osoby do bieżącego kontaktu z Zamawiającym.
5. Sposób składania oświadczeń i dokumentów w ofercie wspólnej:
  - a) **oferta** – składa pełnomocnik wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, jako jeden dokument, w imieniu wszystkich Wykonawców;
  - b) **JEDZ** - składa we własnym imieniu każdy z wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego,
  - c) **oświadczenie o przynależności/braku przynależności do grupy kapitałowej** - składa we własnym imieniu każdy z wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego,
  - d) **oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia** - składa we własnym imieniu każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego,
  - e) **oświadczenia i dokumenty potwierdzające spełnianie warunków udziału w postępowaniu** – składa pełnomocnik Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, w imieniu wszystkich Wykonawców, jako jeden dokument, tj. wykaz dostaw wraz z dowodami należytego wykonania.
6. Przed podpisaniem umowy (w przypadku wygrania przetargu) Wykonawcy składający ofertę wspólną będą mieli obowiązek przedstawić Zamawiającemu umowę regulującą ich współpracę.
7. Wspólnicy spółki cywilnej są traktowani jak Wykonawcy składający ofertę wspólną i mają do nich zastosowanie zasady określone w niniejszym rozdziale.

## ROZDZIAŁ IX. Warunki udziału w postępowaniu, dokumenty i oświadczenia żądane przez Zamawiającego, sposób wypełnienia JEDZa, wezwanie do uzupełnienia

1. O udzielenie zamówienia publicznego mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12)-23) oraz art. 24 ust. 5 pkt 1) i 8) ustawy pzp.
2. O udzielenie zamówienia publicznego mogą ubiegać się Wykonawcy, którzy posiadają doświadczenie w postaci należytego wykonania w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, przynajmniej jednej usługi, odpowiadającej przedmiotowi zamówienia, o wartości równej lub przekraczającej 100 000,00 zł brutto. Za usługę odpowiadającą przedmiotowi zamówienia Zamawiający uzna usługę, polegającą na wdrożeniu systemu ochrony poczty elektronicznej zapewniającego kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową.

W przypadku ofert wspólnych doświadczeniem musi wykazać się jeden z wykonawców składających ofertę wspólną. Zamawiający nie dopuszcza łączenia doświadczeń, w celu wspólnego wykazania spełniania warunku udziału w postępowaniu.

3. Wykonawca zobowiązany jest złożyć wraz z ofertą wstępne oświadczenie, w formie JEDZ, wypełniony w zakresie wskazanym przez zamawiającego w ogłoszeniu o zamówieniu i w specyfikacji istotnych warunków zamówienia.
4. Zamawiający przedkłada w załączeniu wzór oświadczenia JEDZ, opracowany w oparciu o formularz ustanowiony w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust 3 dyrektywy 2014/25/UE:
  - a) zamawiający udostępnia wypełniony w żądanym zakresie JEDZ na stronie internetowej, w formie pliku xlm. Pliku nie należy otwierać lecz pobrać go na komputer,
  - b) w celu wypełnienia JEDZa przez wykonawcę lub inne podmioty należy wejść na stronę <https://ec.europa.eu/tools/espd/filter?lang=pl>, wybrać pole „jestem wykonawcą”, a następnie zaznaczyć pole „zaimportować ESPD”. Poniżej należy wczytać plik JEDZa, umieszczony w lokalizacji fizycznej na dysku lokalnym wykonawcy i kliknąć przycisk „Dalej”. Zaimportowany JEDZ należy wypełnić wyłącznie w zakresie przygotowanym przez Zamawiającego i podpisać kwalifikowanym podpisem elektronicznym,
  - c) **Zamawiający prosi, by wykonawca w części IV JEDZa wypełnił jedynie sekcję  $\alpha$  (alfa) i nie wypełniał żadnej z pozostałych sekcji w części IV,**
  - e) Wykonawca może wykorzystać w JEDZ nadal aktualne informacje zawarte w innym JEDZ, złożonym w odrębnym postępowaniu o udzielenie zamówienia,
  - f) w przypadku wspólnego ubiegania się o zamówienie przez wykonawców, JEDZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie,
  - g) w przypadku gdy wykonawca powołuje się przy spełnieniu warunków udziału w postępowaniu na zasoby innych podmiotów zobowiązany jest złożyć JEDZe dotyczące każdego z nich – w zakresie niezbędnym do wykazania braku podstaw do wykluczenia oraz spełnienia warunków udziału w postępowaniu w odniesieniu do udostępnianego potencjału.
5. Na potwierdzenie braku podstaw do wykluczenia wykonawca, którego oferta zostanie najwyższej oceniona, na wezwanie zamawiającego, złoży w wyznaczonym terminie, aktualne na dzień złożenia następujące oświadczenia i dokumenty:
  - 1) informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy PZP, wystawioną nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
  - 2) oświadczenia wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku





- wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności;
- 3) oświadczenia wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne;
  - 4) odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy PZP.
  - 5) zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
  - 6) zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
  - 7) oświadczenia wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2016 r. poz. 716).  
W przypadku ofert wspólnych dokumenty/oświadczenia składa każdy z Wykonawców składających ofertę wspólną.  
W przypadku polegania na zdolnościach podmiotów trzecich, Wykonawca przedstawia także ww. oświadczenia/dokumenty dotyczące tych podmiotów.
  - 8) brak podstaw do wykluczenia z przesłanki opisanej w art. 24 ust. 1 pkt 23) pzp Wykonawca potwierdza składając, w terminie 3 dni od dnia zamieszczenia przez Zamawiającego na stronie internetowej informacji z otwarcia ofert, oświadczenie o braku przynależności do grupy kapitałowej lub oświadczenie o przynależności do grupy kapitałowej z załączeniem dowodów potwierdzających, że występujące w postępowaniu powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji.



W przypadku ofert wspólnych oświadczenie o przynależności/braku przynależności do grupy kapitałowej i ewentualne dowody na brak zakłócenia konkurencji składa każdy z Wykonawców składających ofertę wspólną.

Dokumenty mogą być złożone w oryginale, w postaci dokumentów elektronicznych podpisanych kwalifikowanym podpisem elektronicznym lub w elektronicznej kopii dokumentu/oświadczenia, poświadczonej za zgodność z oryginałem kwalifikowanym podpisem elektronicznym.

Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot na którego zdolnościach polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą. Jeżeli poświadczenia dokonuje pełnomocnik, z treści pełnomocnictwa musi wyraźnie wynikać upoważnienie do tej czynności.

6. Wykonawcy zagraniczni:

1) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa:

- a) w ust. 3 pkt 1) niniejszego rozdziału składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy PZP;
- b) w ust. 3 pkt 4)-6) niniejszego rozdziału, składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

- nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
- nie otwarto jego likwidacji ani nie ogłoszono upadłości.

2) Dokumenty, o których mowa w ust. 4 pkt 1) lit. a) i b) tiret drugi, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w ust. 4 pkt 1) lit. b) tiret pierwszy, powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

3) Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 1), zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób

- uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby, z zachowaniem terminów o których mowa w pkt 2) niniejszego ustępu.
- 4) Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w ust. 3 pkt 1), składa dokument, o którym mowa w pkt 1 lit. a), w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy PZP. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby, z zachowaniem terminów o których mowa w pkt 2) niniejszego ustępu.
  - 5) W przypadku wątpliwości co do treści dokumentu złożonego przez wykonawcę, zamawiający może zwrócić się do właściwych organów kraju, w którym miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.
7. Na potwierdzenie spełniania warunków udziału w postępowaniu wykonawca, którego oferta zostanie najwyżej oceniona, na wezwanie zamawiającego, złoży w wyznaczonym terminie aktualny na dzień złożenia wykaz usług, wykonanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane wraz z załączeniem dowodów określających czy te usługi zostały wykonane należycie. Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy;  
W przypadku ofert wspólnych wykaz usług składa pełnomocnik wykonawców wspólnie ubiegających się o udzielenie zamówienia.

W przypadku dostarczenia przez wykonawców dokumentów dotyczących warunków udziału w postępowaniu, w których wartości zostały podane w walutach obcych, Zamawiający w celu dokonania oceny spełnienia warunków uczestnictwa w postępowaniu dokona przeliczenia podanych wartości po średnim kursie ogłoszonym przez Narodowy Bank Polski obowiązującym na dzień, w którym w Dzienniku Urzędowy Unii Europejskiej zostało opublikowane ogłoszenie o zamówieniu.

Dokumenty lub oświadczenia, o których mowa w rozporządzeniu o dokumentach, sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

## ROZDZIAŁ X. Wadium i sposób jego wniesienia

1. Wykonawca przystępujący do przetargu jest zobowiązany wnieść wadium w wysokości: **5.000,00 zł (słownie złotych: pięć tysięcy).**
2. Wniesione wadium musi obejmować cały okres związania ofertą.
3. Wadium może być wniesione według wyboru wykonawcy w pieniądzu, poręczeniach bankowych, gwarancjach bankowych, gwarancjach ubezpieczeniowych poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tj. Dz. U. z 2016 r. poz. 359 ze zm.).
4. Wadium wnoszone w formie pieniężnej należy wpłacić na konto PUM w Szczecinie – Santander Bank Polska S.A. III O/Szczecin 06 1090 1492 0000 0001 0053 7752 z dopiskiem: „**wadium: DZP-262-7/2019 – System ochrony poczty elektronicznej pracowników PUM**”, przed upływem terminu składania ofert.
5. Wadium wnoszone w formie niepieniężnej musi zostać wniesione wraz z ofertą w oryginale, w postaci elektronicznej.
6. Wadium wniesione w formie innej niż pieniężna musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez wykonawcę określone w ustawie Prawo zamówień publicznych.
7. Zamawiający zwraca wadium wszystkim wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem wykonawcy, którego oferta została wybrana jako najkorzystniejsza.
8. Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, zamawiający zwraca wadium niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego.
9. Zamawiający zwraca niezwłocznie wadium na wniosek wykonawcy, który wycofał ofertę przed upływem terminu składania ofert.
10. Zamawiający żąda ponownego wniesienia wadium przez wykonawcę, któremu zwrócono wadium, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez zamawiającego.
11. Jeżeli wadium wniesiono w pieniądzu, zamawiający zwraca je wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez wykonawcę.
12. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli:
  - 1) wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a ustawy PZP, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów



potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, oświadczenia, o którym mowa w art. 25a ust. 1 ustawy PZP, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy PZP, co spowodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej;

- 2) wykonawca, którego oferta została wybrana odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;
- 3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie wykonawcy.

## ROZDZIAŁ XI. Kryteria oceny ofert i opis sposobu oceny ofert

1. Zamawiający przy wyborze najkorzystniejszej oferty będzie się kierował następującymi kryteriami:

<i>Lp.</i>	<i>Kryterium</i>	<i>Ranga</i>
1	<p><b>CENA</b></p> <p>Wartość punktowa jest obliczana wg wzoru:</p> $R \cdot \frac{C_n}{C_b} \times 100 \times 60\%$ <p>gdzie:</p> <p><b>R</b> – ranga ocenianego kryterium  <b>C<sub>n</sub></b> - cena najniższa  <b>C<sub>b</sub></b> - cena badana</p> <p>W tym kryterium wykonawca może otrzymać maksymalnie 60 punktów.</p>	60%
2	<p>Parametry techniczne</p> <p>Zamawiający przyzna ofertom punktację za parametr:</p> <p>„Obsługiwana przestrzeń”: minimum 3 TB - 0 pkt.  minimum 3,5 TB - 10 pkt.  minimum 4 TB - 20 pkt.</p> <p>oraz</p> <p>„Wydajność skanowania”: minimum 180 tys./godz. - 0 pkt.  minimum 200 tys./godz. - 5 pkt.  minimum 220 tys./godz. - 10 pkt.</p>	30%



	<p>Wartość punktowa w tym kryterium zostanie następnie obliczona wg</p> $R \cdot \frac{P_n}{P_{\max}} \times 100 \times 30\%$ <p>wzoru: gdzie:</p> <p><b>R</b> – ranga ocenianego kryterium, <b>P<sub>n</sub></b> – suma punktów w badanej ofercie, <b>P<sub>max</sub></b> – najwyższa suma punktów.</p> <p>W tym kryterium wykonawca może otrzymać maksymalnie 30 punktów.</p>	
3	<p>Termin dostawy kodów licencyjnych</p> <p>Za zaoferowanie dostarczenia kodów licencyjnych w terminie: 30 dni - 0 pkt 20 dni - 10 pkt.</p> <p>W tym kryterium wykonawca może otrzymać maksymalnie 10 punktów.</p>	10%

- Zamawiający informuje, że maksymalny czas dostawy kodów licencyjnych nie może być dłuższy niż 30 dni od daty podpisania umowy. Zaoferowanie czasu dostarczenia kodów licencyjnych dłuższego niż 30 dni spowoduje odrzucenie oferty na podstawie art. 89 ust.1 pkt 2) ustawy p.z.p.
- Zaoferowanie przez Wykonawcę czasu dostarczenia kodów licencyjnych krótszego niż 20 dni spowoduje przyznanie takiej samej ilości punktów jak za 20 dni. Zaoferowanie w ofercie czasu dostarczenia kodów licencyjnych dłuższego niż 20 dni spowoduje przyznanie takiej samej ilości punktów jak za 30 dni.

## ROZDZIAŁ XII. Opis sposobu obliczania ceny oraz rozliczenia z wykonawcą

- Wykonawca, składając ofertę poda cenę w PLN, zawierającą także stawkę podatku VAT.
- Cena powinna zawierać w sobie ewentualne upusty proponowane przez Wykonawcę (niedopuszczalne są żadne negocjacje cenowe).
- W cenie wykonawca ujmie wszelkie koszty związane z realizacją zamówienia, w szczególności koszty związane z:
  - udzielaniem kompleksowego wsparcia technicznego w zakresie instalacji systemu, jego konfiguracji oraz uruchomienia na produkcji, na platformie wskazanej przez Zamawiającego,
  - wsparciem technicznym pierwszego kontaktu w języku polskim świadczonym przez inżynierów certyfikowanych (w przypadku produktu firmy Fortinet wymagany jest certyfikat NSE 4), za pośrednictwem poczty elektronicznej oraz poprzez pomoc zdalną,

- 3) zakładaniem zgłoszeń serwisowych u producenta,
  - 4) doradztwem w zakresie konfiguracji,
  - 5) rekonfiguracją systemu ochrony poczty z uwagi na zmianę środowiska pracy (do 10 zgłoszeń),
  - 6) 2-dniowym (2 x 8 godzin zegarowych) szkoleniem dla 2 administratorów w lokalizacji Zamawiającego.
4. Jeżeli złożono ofertę, której wybór prowadziłby do powstania obowiązku podatkowego zamawiającego, zgodnie z przepisami o podatku od towarów i usług w zakresie wewnątrz wspólnotowego nabycia towarów, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami. Informację o tym wykonawca podaje w ofercie.
5. Rozliczenia między Zamawiającym, a Wykonawcą prowadzone będą w walucie polskiej. Zamawiający nie dopuszcza możliwości prowadzenia rozliczeń w walucie obcej.

### **ROZDZIAŁ XIII. Postępowanie po otwarciu ofert, ocena ofert i wybór najkorzystniejszej oferty**

1. Zamawiający za najkorzystniejszą uzna ofertę tego wykonawcy, który uzyska najkorzystniejszy bilans punktów na podstawie kryteriów określonych w SIWZ.
2. Przed udzieleniem zamówienia wykonawca, którego oferta została najwyżej oceniona zostanie wezwany do złożenia w wyznaczonym terminie aktualnych dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, w zakresie wynikającym z treści SIWZ oraz ogłoszenia o zamówieniu.
3. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych dokumentów potwierdzających, że nie podlegają wykluczeniu i spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio dokumenty nie są już aktualne, do złożenia aktualnych dokumentów.
4. Jeżeli wykonawca nie złoży oświadczenia, o których mowa w art. 25a ust. 1 ustawy PZP, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez zamawiającego wątpliwości, zamawiający wezwie do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień, w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
5. Jeżeli wykonawca nie złoży wymaganych pełnomocnictw albo złoży wadliwe pełnomocnictwa, zamawiający wezwie do ich złożenia w terminie przez siebie

wskazanych, chyba że mimo ich złożenia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

6. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Niedopuszczalne jest prowadzenie między zamawiającym, a wykonawcą negocjacji dotyczących złożonej oferty.

## ROZDZIAŁ XIV. Termin wykonania zamówienia, gwarancja i wsparcie

1. Wykonawca jest zobowiązany do dostarczenia kodu lub kodów licencyjnych najpóźniej w ciągu 30 dni od daty podpisania umowy.
2. Wykonawca zobowiązany do wdrożenia systemu na produkcji na platformie wskazanej przez Zamawiającego w ciągu 3 miesięcy od daty podpisania umowy.
3. System musi być objęty gwarancyjnym pakietem usług producenta przez okres 36 miesięcy, upoważniającym do:
  - aktualizacji oprogramowania (kontrola antyspam, URL Filtering i kontrola antywirusowa) w ramach dostarczonych licencji,
  - wsparcia technicznego, które musi być świadczone w trybie 24x7 z czasami reakcji opisanymi poniżej.

Definicje priorytetów zdarzeń		
Priorytet	Ogólna definicja zdarzenia	Przykłady
Priorytet 1	Każde zgłoszenie problemu, który powoduje całkowitą lub ciągłą niestabilność funkcji krytycznych uniemożliwiającą pracę systemu w środowisku produkcyjnym.	<ul style="list-style-type: none"> <li>• Utrata dostępu do usług.</li> <li>• Katastrofalny wpływ na funkcjonalności krytyczne w środowisku produkcyjnym.</li> <li>• Przerwa w działaniu wpływająca na sesje aktywne lub ruch o znaczeniu krytycznym.</li> <li>• Istotna luka w bezpieczeństwie wpływająca na aktywne usługi biznesowe itp.</li> </ul>
Priorytet 2	Każde zgłoszenie problemu, który ma znaczący wpływ na funkcjonalności krytyczne systemu w środowisku produkcyjnym.	<ul style="list-style-type: none"> <li>• Częste niestabilności funkcji krytycznych, mające wpływ na aktywne sesje użytkowników w środowisku produkcyjnym.</li> <li>• Utrata nadmiarowości krytycznego składnika wpływającego na usługi biznesowe.</li> </ul>
Priorytet 3	Zgłoszenie problemu który ma minimalny wpływ na funkcjonalności krytyczne systemu w środowisku produkcyjnym.	<ul style="list-style-type: none"> <li>• Sporadyczne niestabilności funkcji podstawowych.</li> </ul>
Priorytet 4	Zgłoszenia tworzone w celu pozyskania dodatkowych informacji, pomocy w konfiguracji oraz dotyczące drobnych usterek.	<ul style="list-style-type: none"> <li>• Dodanie do konfiguracji dodatkowego filtrowania wykorzystującego bazę Bayesa.</li> </ul>

Czasy reakcji serwisu producenta		
Priorytet	Maksymalny dopuszczalny czas	Maksymalny dopuszczalny czas



	odpowiedzi początkowej	reakcji na kolejne odpowiedzi klienta
Priorytet 1	mniej niż 1 godzina	co 6 godzin
Priorytet 2	mniej niż 1 godzina	1 dzień
Priorytet 3	następny dzień roboczy	co 3 dni robocze
Priorytet 4	2 następne dni robocze	1 tydzień

4. Wykonawca zagwarantuje:

- udzielenie kompleksowego wsparcia technicznego w zakresie instalacji systemu, jego konfiguracji oraz uruchomienia na produkcji, na platformie wskazanej przez Zamawiającego.
- wsparcie techniczne pierwszego kontaktu w języku polskim świadczone przez inżynierów certyfikowanych (np. w przypadku produktu firmy Fortinet wymagany jest certyfikat NSE 4), za pośrednictwem poczty elektronicznej oraz poprzez pomoc zdalną,
- zakładanie zgłoszeń serwisowych u producenta.
- doradztwo w zakresie konfiguracji.
- rekonfigurację systemu ochrony poczty z uwagi na zmianę środowiska pracy (do 10 zgłoszeń).
- 2-dniowe (2 x 8 godzin zegarowych) szkolenie dla 2 administratorów w lokalizacji Zamawiającego.

## ROZDZIAŁ XV. Zawarcie umowy o zamówienie publiczne

1. W przypadku dokonania wyboru oferty najkorzystniejszej z wykonawcą zostanie zawarta umowa o udzielenie zamówienia publicznego.
2. Zamawiający zawrze umowę w sprawie zamówienia publicznego, z zastrzeżeniem art. 183 ustawy w terminie nie krótszym niż 10 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, chyba że w postępowaniu zostanie złożona tylko jedna oferta.
3. Jeżeli wykonawca, którego oferta została wybrana uchyla się od zawarcia umowy, zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu wykonawca, który złożył ofertę najwyższej ocenioną spośród pozostałych ofert.

## ROZDZIAŁ XVI. Środki ochrony prawnej

1. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy PZP czynności zamawiającego, podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy pzp.

2. Odwołanie powinno wskazywać czynność lub zaniechanie czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
3. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
4. Odwołujący przesyła kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Domniemywa się, iż zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
5. Odwołanie wnosi się w terminie 10 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia.
6. Odwołanie wobec treści ogłoszenia o zamówieniu oraz wobec postanowień specyfikacji istotnych warunków zamówienia, wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia specyfikacji istotnych warunków zamówienia na stronie internetowej.
7. Odwołanie wobec czynności innych niż określone w ust. 6 wnosi się terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.
9. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
10. Skargę wnosi się do Sądu Okręgowego właściwego dla siedziby Zamawiającego, czyli do Sądu Okręgowego w Szczecinie, VIII Wydział Gospodarczy przy ul. Małopolskiej 17, 70-952 Szczecin.
11. Skargę wnosi się za pośrednictwem Prezesa Krajowej Izby Odwoławczej w terminie 7 dni od dnia doręczenia orzeczenia Izby, przysyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora publicznego jest równoznaczne z jej wniesieniem.
12. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego właściwemu sądowi w terminie 7 dni od dnia jej otrzymania.
13. Sąd rozpoznaje sprawę niezwłocznie, nie później jednak niż w terminie 1 miesiąca od dnia wpływu skargi do sądu.
14. Od wyroku sądu lub postanowienia kończącego postępowanie w sprawie nie przysługuje skarga kasacyjna.

## ROZDZIAŁ XVII. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest usługa wdrożenia systemu ochrony poczty elektronicznej zapewniającego kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową, według parametrów podanych poniżej:

Wymaganie (cecha / funkcjonalność)	Parametr	Ocena / punktacja
<b>1. WYMAGANIA OGÓLNE</b>		
System ochrony poczty elektronicznej musi być zrealizowany w postaci wirtualnej platformy, która musi posiadać możliwość uruchomienia na niżej wymienionych hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.		
System musi pracować pod kontrolą dedykowanego systemu operacyjnego oraz wykorzystywać aktualizowane na bieżąco bazy zabezpieczeń.		
System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.		
System musi mieć możliwość pracy w następujących trybach: Gateway Serwer <ul style="list-style-type: none"> <li>• Transparentny (rekonfiguracja używanego systemu poczty elektronicznej nie jest w tym przypadku wymagana).</li> </ul>		
System musi obsługiwać co najmniej 6 interfejsów sieciowych.		
System musi obsługiwać przestrzeń dyskową o pojemności co najmniej 3 TB	Obsługiwana przestrzeń	minimum 3 TB minimum 3,5 TB minimum 4 TB
System musi realizować skanowanie antyspamowe oraz antywirusowe z wydajnością minimum 180 tysięcy wiadomości/godzinę.	Wydajność skanowania	minimum 180 tys./godz. minimum 200 tys./godz. minimum 220 tys./godz.
System musi umożliwiać zapisanie konfiguracji systemu w pliku (lub plikach) na nośniku zewnętrznym, z możliwością jej późniejszego odtworzenia.		
System ochrony poczty musi być przystosowany do aktywnej współpracy oraz wymiany informacji z firewall posiadany przez Zamawiającego (Fortigate), w ramach kompatybilnych mechanizmów o wykrytych podatnościach.		



<b>2. TRYB GATEWAY / TRANSPARENTNY</b>		
<p><b>Funkcje ogólne</b></p> <p>Dostarczany system ochrony poczty musi zapewniać poniższe funkcje:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla co najmniej 800 domen pocztowych.</li> <li>• Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).</li> <li>• Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.</li> <li>• Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).</li> <li>• Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.</li> <li>• Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.</li> <li>• Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.</li> <li>• Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.</li> <li>• Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.</li> <li>• Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.</li> <li>• Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.</li> <li>• Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.</li> <li>• Ochrona przed wyciekami informacji poufnej DLP (Data Leak Prevention).</li> </ul>		
<p><b>Kontrola antywirusowa i ochrona przed malware</b></p> <p>W ww. zakresie dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> <li>• Skanowanie antywirusowe wiadomości SMTP.</li> <li>• Kwarantannę dla zainfekowanych plików.</li> <li>• Skanowanie załączników skompresowanych.</li> <li>• Definiowanie komunikatów powiadomień w języku polskim.</li> <li>• Blokowanie załączników w oparciu o typ pliku.</li> <li>• Możliwość zdefiniowania nie mniej niż 800 polityk kontroli antywirusowej.</li> <li>• Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną platformą (sprzętową lub wirtualną) lub</li> </ul>		



<p>usługą w chmurze typu Sandbox w celu rozpoznawania nieznanymi dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.</p> <ul style="list-style-type: none"> <li>Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.</li> </ul>		
<p><b>Kontrola antyspamowa</b> System musi zapewniać poniższe funkcje i metody filtrowania spamu:</p> <ul style="list-style-type: none"> <li>Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.</li> <li>Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.</li> <li>Szczegółowa kontrola nagłówka wiadomości.</li> <li>Analiza Heurystyczna.</li> <li>Współpraca z zewnętrznymi serwerami RBL, SURBL.</li> <li>Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.</li> <li>Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.</li> <li>Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.</li> <li>Kontrola w oparciu o Greylisting oraz SPF.</li> <li>Filtrowanie treści wiadomości i załączników.</li> <li>Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.</li> <li>Możliwość zdefiniowania nie mniej niż 800 polityk kontroli antyspamowej.</li> <li>Ochrona typu outbrake.</li> <li>Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).</li> <li>Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora..</li> </ul>		
<p><b>Ochrona przed atakami na usługę poczty</b> System musi zapewniać poniższe funkcje i metody filtrowania:</p>		

<ul style="list-style-type: none"> <li>• Ochrona przed atakami na adres odbiorcy.</li> <li>• Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.</li> <li>• Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.</li> <li>• Kontrola Reverse DNS (ochrona przed Anty-Spoofing).</li> <li>• Weryfikacja poprawności adresu e-mail nadawcy.</li> </ul>		
<p><b>Funkcje logowania i raportowania</b> W ww. zakresie dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> <li>• Logowanie do zewnętrznego serwera SYSLOG.</li> <li>• Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.</li> <li>• Logowanie informacji na temat spamu oraz niedozwolonych załączników.</li> <li>• Możliwość podglądu logów w czasie rzeczywistym.</li> <li>• Możliwość analizy przebiegu sesji SMTP.</li> <li>• Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.</li> <li>• Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.</li> <li>• Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.</li> </ul>		
<b>3.TRYB SERWER</b>		
<p><b>Funkcje serwera poczty</b> W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiającą zdefiniowanie co najmniej 1500 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP, obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.</p> <p>Ponadto w ww. zakresie dostarczony system musi zapewniać:</p> <ul style="list-style-type: none"> <li>• Obsługę serwisów pocztowych: SMTP, POP3, IMAP.</li> <li>• Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).</li> <li>• Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.</li> </ul>		

<ul style="list-style-type: none"> <li>• Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).</li> <li>• Polski interfejs użytkownika przy dostępie przez WebMail.</li> <li>• Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.</li> <li>• Uwierzytelnianie użytkowników w oparciu o: bazę lokalną oraz Radius.</li> </ul>		
<p><b>Funkcje ogólne systemu ochrony poczty</b> Dostarczany system ochrony poczty musi zapewniać obsługę poniższych funkcji:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla co najmniej 800 domen pocztowych.</li> <li>• Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).</li> <li>• Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.</li> <li>• Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).</li> <li>• Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.</li> <li>• Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.</li> <li>• Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.</li> <li>• Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.</li> <li>• Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.</li> <li>• Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.</li> <li>• Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.</li> <li>• Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.</li> <li>• Białe i czarne listy adresów mailowych dla</li> </ul>		



<p>poszczególnych użytkowników.</p> <ul style="list-style-type: none"> <li>• Ochrona przed wyciekami informacji poufnej DLP (Data Leak Preention)</li> </ul>		
<p><b>Kontrola antywirusowa i ochrona przed malware</b></p> <p>W ww. zakresie dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> <li>• Skanowanie antywirusowe wiadomości SMTP.</li> <li>• Kwarantannę dla zainfekowanych plików.</li> <li>• Skanowanie załączników skompresowanych.</li> <li>• Definiowanie komunikatów powiadomień w języku polskim.</li> <li>• Blokowanie załączników w oparciu o typ pliku.</li> <li>• Możliwość zdefiniowania nie mniej niż 800 polityk kontroli antywirusowej.</li> <li>• Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanymi dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.</li> <li>• Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.</li> </ul>		
<p><b>Kontrola antyspamowa</b></p> <p>System musi zapewniać obsługę poniższych funkcji oraz metod filtrowania spamu:</p> <ul style="list-style-type: none"> <li>• Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.</li> <li>• Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.</li> <li>• Szczegółowa kontrola nagłówka wiadomości.</li> <li>• Analiza Heurystyczna.</li> <li>• Współpraca z zewnętrznymi serwerami RBL, SURBL.</li> <li>• Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.</li> <li>• Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.</li> <li>• Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF.</li> </ul>		





<ul style="list-style-type: none"> <li>• Kontrola w oparciu o Greylisting oraz SPF.</li> <li>• Filtrowanie treści wiadomości i załączników.</li> <li>• Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.</li> <li>• Możliwość zdefiniowania nie mniej niż 800 polityk kontroli antyspamowej.</li> <li>• Ochrona typu outbrake.</li> <li>• Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).</li> <li>• Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.</li> </ul>		
<p><b>Ochrona przed atakami na usługę poczty</b> System musi zapewniać obsługę poniższych funkcji oraz metod filtrowania:</p> <ul style="list-style-type: none"> <li>• Ochrona przed atakami na adres odbiorcy.</li> <li>• Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.</li> <li>• Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.</li> <li>• Kontrola Reverse DNS (ochrona przed Anty-Spoofing).</li> <li>• Weryfikacja poprawności adresu e-mail nadawcy.</li> </ul>		
<p><b>Funkcje logowania i raportowania</b> W tym zakresie dostarczony system ochrony poczty musi zapewniać:</p> <ul style="list-style-type: none"> <li>• Logowanie do zewnętrznego serwera SYSLOG.</li> <li>• Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.</li> <li>• Logowanie informacji na temat spamu oraz niedozwolonych załączników.</li> <li>• Możliwość podglądu logów w czasie rzeczywistym.</li> <li>• Możliwość analizy przebiegu sesji SMTP.</li> <li>• Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.</li> <li>• Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.</li> <li>• Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie</li> </ul>		



administratora systemu.		
<b>4. PRACA W TRYBIE WYSOKIEJ DOSTĘPNOŚCI (HA)</b>		
System ochrony poczty musi zapewniać obsługę poniższych funkcji: <ul style="list-style-type: none"> <li>• Konfigurację HA w trybach: Gateway oraz Transparent.</li> <li>• Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urzędzeń występuje pod innym adresem IP.</li> <li>• Wykrywanie awarii poszczególnych urzędzeń oraz powiadamianie administratora systemu.</li> <li>• Monitorowanie stanu pracy klastra.</li> </ul>		
<b>5. AKTUALIZACJE SYGNATUR, DOSTĘP DO BAZY SPAMU</b>		
W ww. zakresie dostarczony system ochrony poczty musi zapewniać: <ul style="list-style-type: none"> <li>• Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.</li> <li>• Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.</li> </ul>		
<b>6. ZARZĄDZANIE</b>		
System ochrony poczty musi zapewniać obsługę poniższych funkcji: <ul style="list-style-type: none"> <li>• System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.</li> <li>• Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.</li> <li>• Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.</li> </ul>		
<b>7. GWARANCJA ORAZ WSPARCIE</b>		
System musi być objęty gwarancyjnym pakietem usług producenta przez okres 36 miesięcy, upoważniającym do: <ul style="list-style-type: none"> <li>• częściowych aktualizacji oprogramowania (tzw. udpate – obejmujący kontrolę antyspamu, URL Filtering i kontrolę antywirusową) w ramach dostarczonych licencji,</li> <li>• aktualizacji oprogramowania do bieżącej wersji stabilnej (tzw. udgrade ),</li> <li>• wsparcia technicznego, które musi być świadczone w trybie 24x7 z czasami reakcji opisanymi w Rozdziale XIV ust. 3 niniejszej siwz</li> </ul> <p>Wykonawca ze swojej strony gwarantuje:</p> <ul style="list-style-type: none"> <li>• Udzielenia kompleksowego wsparcia technicznego w zakresie instalacji systemu, jego konfiguracji oraz uruchomienia na produkcji, na platformie wskazanej przez</li> </ul>		

<p>Zamawiającego.</p> <ul style="list-style-type: none"> <li>• Wsparcie techniczne pierwszego kontaktu w języku polskim świadczone przez inżynierów certyfikowanych (w przypadku produktu firmy Fortinet wymagany jest certyfikat NSE 4), za pośrednictwem poczty elektronicznej oraz poprzez pomoc zdalną),</li> <li>• Zakładanie zgłoszeń serwisowych u producenta.</li> <li>• Doradztwo w zakresie konfiguracji.</li> <li>• Rekonfiguracja systemu ochrony poczty z uwagi na zmianę środowiska pracy (do 10 zgłoszeń).</li> <li>• 2-dniowe (2x8 godzin zegarowych) szkolenie dla 2 administratorów w lokalizacji Zamawiającego.</li> </ul>		
<b>8. ŹRÓDŁO POZYSKANIA PRODUKTU</b>		
<ul style="list-style-type: none"> <li>• Produkt musi zostać zakupiony w oficjalnym kanale sprzedaży producenta.</li> <li>• Wykonawca powinien przedłożyć przed podpisaniem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta, potwierdzające autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</li> </ul>		
<b>9. TERMIN DOSTARCZENIA KODÓW LICENCYJNYCH</b>		
<p>Wykonawca jest zobowiązany do dostarczenia kodu lub kodów licencyjnych najpóźniej w ciągu 30 dni od daty podpisania umowy</p>	<p>Czas dostarczenia kodów licencyjnych</p>	<p>30 dni 20 dni</p>
<b>10. TERMIN WDROŻENIA SYSTEMU</b>		
<p>Wykonawca zobowiązany do wdrożenia systemu na produkcji na platformie wskazanej przez Zamawiającego w ciągu 3 miesięcy od daty podpisania umowy</p>		

4. Miejscem wdrożenia i szkolenia jest budynek Pomorskiego Uniwersytetu Medycznego w Szczecinie, ul. Rybacka 1, 70-204 Szczecin.
5. Na podstawie art. 29 ust. 3a ustawy pzp zamawiający wymaga zatrudnienia przez wykonawcę i każdego podwykonawcę na podstawie umowy o pracę osób wykonujących czynności w zakresie realizacji zamówienia, jeżeli wykonanie tych czynności polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2016 r. poz. 1666, 2138 i 2255 oraz z 2017 r. poz. 60 i 962). Wymóg ten dotyczy osób, które wykonują czynności bezpośrednio związane z wykonywaniem usług, w szczególności związanych z wdrożeniem systemu, wsparciem technicznym, doradztwem, szkoleniem pracowników Zamawiającego.
6. Zamawiający, w trakcie realizacji zamówienia, zastrzega sobie prawo do wrywkowego dokonywania kontroli zatrudniania na umowy o pracę osób, wykonujących czynności związanych z realizacją zamówienia. W celu kontroli zamawiający skieruje do wykonawcy żądanie udowodnienia zamawiającemu w terminie 2 dni od dnia otrzymania przez wykonawcę żądania zamawiającego, za pomocą dowolnych, dostępnych

- wykonawcy środków dowodowych faktu zatrudniania wskazanych osób na umowy o pracę.
7. W trakcie realizacji zamówienia na każde wezwanie zamawiającego, w wyznaczonym w tym wezwaniu terminie, wykonawca przedłoży zamawiającemu wskazane poniżej dowody w celu potwierdzenia spełnienia wymogu zatrudnienia na podstawie umowy o pracę przez wykonawcę lub podwykonawcę osób wykonujących wskazane w ust. 3 czynności w trakcie realizacji zamówienia:
    - oświadczenie wykonawcy lub podwykonawcy o zatrudnieniu na podstawie umowy o pracę osób wykonujących czynności, których dotyczy wezwanie zamawiającego. Oświadczenie to powinno zawierać w szczególności: dokładne określenie podmiotu składającego oświadczenie, datę złożenia oświadczenia, wskazanie, że objęte wezwaniem czynności wykonują osoby zatrudnione na podstawie umowy o pracę wraz ze wskazaniem liczby tych osób, imion i nazwisk tych osób, rodzaju umowy o pracę i wymiaru etatu oraz podpis osoby uprawnionej do złożenia oświadczenia w imieniu wykonawcy lub podwykonawcy;
    - poświadczoną za zgodność z oryginałem odpowiednio przez wykonawcę lub podwykonawcę kopię umowy/umów o pracę osób wykonujących w trakcie realizacji zamówienia czynności, których dotyczy ww. oświadczenie wykonawcy lub podwykonawcy (wraz z dokumentem regulującym zakres obowiązków, jeżeli został sporządzony). Kopia umowy/umów powinna zostać zanonimizowana w sposób zapewniający ochronę danych osobowych pracowników, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. w szczególności bez adresów, nr PESEL pracowników). Imię i nazwisko pracownika nie podlega anonimizacji. Informacje takie jak: data zawarcia umowy, rodzaj umowy o pracę i wymiar etatu powinny być możliwe do zidentyfikowania;
    - zaświadczenie właściwego oddziału ZUS, potwierdzające opłacanie przez wykonawcę lub podwykonawcę składek na ubezpieczenia społeczne i zdrowotne z tytułu zatrudnienia na podstawie umów o pracę za ostatni okres rozliczeniowy;
    - poświadczoną za zgodność z oryginałem odpowiednio przez wykonawcę lub podwykonawcę kopię dowodu potwierdzającego zgłoszenie pracownika przez pracodawcę do ubezpieczeń, zanonimizowaną w sposób zapewniający ochronę danych osobowych pracowników, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Imię i nazwisko pracownika nie podlega anonimizacji.
  8. W przypadku powzięcia przez zamawiającego informacji o naruszeniu przez wykonawcę lub podwykonawcę obowiązku zatrudnienia na podstawie umowy o pracę osób, albo w przypadku braku przedstawienia dowodów potwierdzających fakt zatrudnienia na umowy o pracę, zamawiający niezwłocznie zawiadomi o tym fakcie Państwową Inspekcję Pracy, celem podjęcia przez nią stosownego postępowania wyjaśniającego w tej sprawie.
  9. Jeśli Państwowa Inspekcja Pracy stwierdzi brak umów o pracę, osób wskazanych przez zamawiającego, będzie to stanowiło podstawę do naliczenia kar umownych, określonych w umowie o zamówienie publiczne.



**Fundusze Europejskie**  
Wiedza Edukacja Rozwój



**Rzeczpospolita  
Polska**



**Unia Europejska**  
Europejski Fundusz Społeczny



10. Zamawiający ma prawo dokonać kontroli, o której mowa w ust. 4 wielokrotnie podczas trwania umowy o zamówienie publiczne.
11. Dokumentem potwierdzającym odbiór przedmiotu zamówienia jest protokół odbioru.