

Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia
Nr ref. KPFR/IT/1/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

„Świadczenie usług informatycznych (IT, cloud i hosting) dla KPFR sp. z o.o. w Toruniu w 2024 roku”

1. Tryb postępowania

Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego, o którym mowa w art. 275 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, zwanej dalej „ustawą Pzp”.

2. Kody CPV

72000000-5 – Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia;

48800000-6 – Systemy i serwery informacyjne;

72415000-2 – Usługi hostingowe dla stron WWW;

72317000-0 – Usługi przechowywania danych.

3. Przedmiot zamówienia

Zamówienie będzie współfinansowane z Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Fundusze Europejskie dla Kujaw i Pomorza 2021-2027, w projekcie pn. „Proces Przedsiębiorczego Odkrywania na rzecz rozwoju Inteligentnych Specjalizacji regionu”.

Świadczenie usługi informatycznej w modelu IaaS na potrzeby funkcjonowania serwisu www i aplikacji wraz z usługami poczty email i ochroną antywirusową i antyspamową urządzeń końcowych oraz świadczeniem usług informatycznych (IT) na potrzeby KPFR sp. z o.o. w Toruniu w 2024 roku. Wszystkie świadczone usługi powinny zapewniać bezpieczeństwo w zakresie przetwarzania oraz przechowywania danych osobowych zgodnie z wymaganiami RODO¹ oraz zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Zamawiający wymaga od Wykonawcy uruchomienia, wdrożenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej IaaS wraz z zapewnieniem rozwiązań w obszarze bezpieczeństwa i ochrony przed cyberzagrożeniami w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw.

Użyte w niniejszym Opisie Przedmiotu Zamówienia (OPZ) i załącznikach wszelkie nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, procesy charakteryzujące produkt lub usługę, należy rozumieć każdorazowo jak opatrzone dopiskiem „lub równoważne”, z wyjątkiem tych, które opisują zasoby posiadane przez Zamawiającego lub z których Zamawiający

¹ RODO - Ogólnego 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 (Dz. Urz. UE L 119/1 z 04.05.2016 r. z późn.zm.).

obecnie korzysta. Parametry opisane przez Zamawiającego należy traktować jako minimalny poziom parametrów jakościowych i cech użytkowych, który muszą spełnić rozwiązania oferowane przez Wykonawcę. Operowanie nazwami własnymi, znakami towarowymi, normami itd. ma jedynie doprecyzować poziom oczekiwań Zamawiającego.

- 1) Przedmiotem zapytania jest świadczenie usługi hostingu, realizację kompleksowej usługi chmury obliczeniowej IaaS (usługi cloud) wraz z usługą wsparcia informatycznego, zwanych dalej Usługą, w systemie ciągłym – stałym miesięcznym. Usługa polega na oddaniu do dyspozycji Zamawiającego zasobów informatycznych w postaci m.in.: powierzchni dyskowej, pamięci operacyjnej oraz mocy obliczeniowej z oprogramowaniem lub bez oraz świadczenia usług utrzymaniowych infrastruktury informatycznej i wsparcia IT. Wykonawca zapewnia Zamawiającemu dostępność usługi SLA, rozumianej jako zagwarantowanie parametrów jakościowych sieci należącej do Wykonawcy na najwyższym możliwym poziomie (dostępności, przepustowości, dostępności protokołów itd.) w zakresie dostawy (udostępnienia) serwerów, chmury i platformy hostingowej na poziomie nie niższym niż 99,95% w skali kwartału podczas trwania zamówienia.
- 2) Wykonawca oferuje usługi w oparciu o infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Europejskiego Obszaru Gospodarczego lub obszaru dla którego Komisja Europejska wydała decyzję uznającą odpowiedni stopień ochrony przetwarzania danych osobowych, zgodnie z określonymi przez zamawiającego wymaganiami (pkt 6). Ponadto zapewnia łącza do sieci Internet, infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami potrzebnymi do prawidłowego uruchomienia i działania usługi zgodnie z określonymi parametrami. Wykonawca zapewnia obsługę udostępnionego sprzętu i oprogramowania wraz ze wsparciem administratorów, ochronę przed atakami i instalacją złośliwego oprogramowania.
- 3) W zakres zadań utrzymaniowych infrastruktury informatycznej i wsparcia IT należy bieżąca obsługa administracyjna zasobów informatycznych wraz z nadzorem nad posiadaną przez Zamawiającego infrastrukturą zlokalizowaną w centrum przetwarzania danych, składającą się w szczególności z zasobów IaaS (Infrastructure as a Service) oraz PaaS (Platform as a Service), poprzez świadczenie usług informatycznych w zakresie:
 - a) migracji usług do infrastruktury;
 - b) instalacji i konfiguracji systemów operacyjnych;
 - c) instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności (HA);
 - d) aktualizacji oprogramowania na życzenie klienta ze względu na błędy bezpieczeństwa;
 - e) wsparcia w utrzymaniu infrastruktury pod kątem wydajności, bezpieczeństwa i optymalizacji kosztowej;
 - f) wsparcia w korzystaniu przez pracowników Zamawiającego w zaproponowanym i wdrożonym przez Wykonawcę środowisku informatycznym do pracy zdalnej,
 - g) wsparcia w realizacji bieżących czynności administracyjnych, w tym również w podstawowym zakresie w obsłudze i zarządzaniu stronami internetowymi należącymi do Zamawiającego, które są umiejscowione (postawione) na udostępnionym w ramach świadczenia Usługi serwerze przez Wykonawcę;
 - h) usługę wykonywania kopii zapasowych, która obejmować będzie wszystkie VM będące składnikami środowiska teleinformatycznego Zamawiającego, oraz wszystkie konta pocztowe, które Wykonawca będzie dostarczał przez cały okres trwania umowy.

Zamawiający oczekuje aby dane cyfrowe kopii zapasowej były gromadzone i przechowywane przez Wykonawcę w sposób bezpieczny w infrastrukturze teleinformatycznej CPD, która spełnia minimalne wymogi bezpieczeństwa opisane w OPZ. Wykonawca zapewni niezbędne licencje i oprogramowanie związane z realizacją zadania. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób zautomatyzowany umożliwi dokonanie na żądanie Zamawiającego odtworzenia kopii zapasowej wybranej VM i weryfikacji spójności wszystkich odtwarzanych danych. Wszelkie zasoby IaaS wraz z oprogramowaniem niezbędnym do odtworzenia kopii zapasowej musi zapewnić Wykonawca. Wykonawca będzie realizował pełne wsparcie eksperckie, merytoryczne i administracyjne w zakresie prawidłowego działania systemu kopii zapasowych i zarządzania całością systemu kopii zapasowych, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres realizacji usługi. Zamawiający oczekuje, aby wszystkie dane były szyfrowane kluczem szyfrującym o długości co najmniej 4096 bit oraz algorytmem szyfrującym powszechnie uznanym za bezpieczny. Usługa backupu dotyczy zarówno komputerów osobistych Zamawiającego jak i serwera Synology o pojemności do 10TB. Zamawiający oczekuje realizacji harmonogramu kopii zapasowych wykonywanych jeden raz dziennie z retencją 7 dni wstecz;

- i) konsultacji wykonawczych z użytkownikami wewnętrznymi i zewnętrznymi;
- j) świadczenia usług doradczych m.in. poprzez udział w pracach związanych z zakupami sprzętu komputerowego, oprogramowania, licencji oraz kontraktów serwisowych, a także współplanowanie rozwoju systemu komputerowego (dobór optymalnych rozwiązań oraz sprzętu);
- k) utrzymania i dostępu do serwera Microsoft Windows Server oraz Microsoft SQL Server 2017 Express;
- l) zagwarantowania jak najszybszego uruchomienia systemu informatycznego w przypadku wystąpienia jakiegokolwiek awarii czy usterki, zarówno występującej w sieci wewnętrznej Wykonawcy, jak i dot. sprzętu (urządzeń) i systemów informatycznych Zamawiającego, w zakresie w jakim wynika to z Umowy, ale nie dłuższym niż 3 dni kalendarzowe;
- m) wydawania zaleceń i opinii dotyczących stanu technicznego i poprawności działania komputerów, sieci i oprogramowania;
- n) współdziałania i obsługi procedur informatycznych związanych z ochroną danych osobowych, w tym dbania o procedury polityki bezpieczeństwa (m.in. stosowania zasad poufności informacji (uniemożliwienie dostępu do danych osobom trzecim), integralności danych, sprawdzania uprawnień użytkowników, szyfrowania danych);
- o) sprawdzania zgodności i ciągłości działania systemów i urządzeń (min. raz na kwartał przeprowadzania testów poprawności działania) i przygotowywania raportów z tych działań na potrzeby Zamawiającego, do 14 dnia miesiąca następującego po zamknięciu danego kwartału. Raporty powinny zawierać przynajmniej następujące dane dotyczące:
 - ataków hakerskich i wycieków danych,
 - przeprowadzonego monitoringu systemów informatycznych,
 - informacje o działaniu połączeń sieciowych i dostępu do dysków sieciowych,
 - wykonanych zadań, w tym przedstawienie czasu realizacji poszczególnych zgłoszonych przez Zamawiającego zadań oraz wskazania źródła ewentualnych awarii (przyczyn ich wystąpienia) oraz przedstawianie osiągniętego poziomu zgodności świadczenia usługi SLA z gwarantowanym przez Wykonawcę poziomem

- w danym okresie. Do obliczenia poziomu gwarantowanego, Zamawiający bierze pod uwagę ilość i długość przerw (liczoną w minutach) świadczenia usługi dostępności (SLA), podaną w danych sprawozdaniach kwartalnych przez Wykonawcę (na podstawie testów poprawności działania SLA) w stosunku do okresu świadczenia usługi przez Wykonawcę w danym kwartale (01.01.2024 r. – 31.03.2024 r. = 91 dni = 131040 minut; 01.04.2024 r. – 30.06.2024 r. = 91 dni = 131040 minut; 01.07.2024 r. – 30.09.2024 r. = 92 dni = 132480 minut; 01.10.2024 r. – 31.12.2024 r. = 92 dni = 132480 minut),
- sprawdzenie kopii zapasowych,
 - testy poprawności działania infrastruktury sprzętowej i sieciowej, w tym do pracy zdalnej, a także stron internetowych Zamawiającego,
 - testy poprawności działania SLA,
- p) wsparcia informatycznego w użytkowanym przez Zamawiającego oprogramowaniu na komputerach Zamawiającego,
- q) wykonawca ma obowiązek dostarczyć oprogramowanie antywirusowe w modelu usługowym na cały okres trwania umowy. Oprogramowanie musi chronić stacje robocze użytkowników oraz maszyny VM Wykonawcy, mieć pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami, wykrywać i usuwać niebezpieczne aplikacje typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
- r) wykonawca ma obowiązek skonfigurować i dostarczyć usługę systemu uprawnień typu Active Directory dla każdego uruchomionego użytkownika końcowego Zamawiającego w ramach zamówienia,
- s) Wykonawca ma obowiązek administrować serwerem Synology mieszczącemu się w siedzibie Zamawiającego, nadawać, modyfikować czy usuwać uprawnienia dostępu użytkowników i grup użytkowników do odpowiednich lokalizacji oraz katalogów i podkatalogów na serwerze Synology,
- t) Wykonawca ma obowiązek administrować serwerem FTP w ramach serwera www.
- 4) Wykonawca świadczyć będzie usługi wsparcia informatycznego, w zależności od potrzeb i zaleceń Zamawiającego, w szczególności poprzez gotowość do świadczenia na odległość, poprzez sieć teleinformatyczną w dni robocze w godzinach 8:00 – 15:30 w wymiarze abonamentowym godzin przypadających na jeden pełen okres rozliczeniowy (zgodnie z parametrami podstawowymi określonymi w pkt 6). Jednocześnie Wykonawca deklaruje realizację dyżuru w trybie 24/7/365 w ramach, którego następuje gotowość do świadczenia Usług na wypadek awarii.
- 5) Wykonawca zobowiązuje się do niezwłocznego usuwania awarii urządzeń w ramach swojej sieci wewnętrznej oraz sprzętu i systemów informatycznych Zamawiającego, za prawidłowe działanie których ponosi odpowiedzialność zgodnie z postanowieniami Umowy. Za awarię uważa się nieprawidłowe działanie jakiegokolwiek urządzenia i systemu, powodujące przerwę w świadczeniu Usług. Wykonawca zobowiązuje się do usuwania awarii w najwcześniejszym możliwym z punktu widzenia technicznego terminie, w normalnym toku czynności, z uwzględnieniem charakteru i rozmiaru awarii, ale nie przekraczającym tygodnia. Standardowy czas reakcji Wykonawcy na zgłoszenie awarii wynosi **nie dłużej niż 3 godz. zegarowe**.

- 6) Wykonawca gwarantuje realizację Usługi na poziomie parametrów podstawowych, tj. w postaci Usługi posiadającej parametry wskazane poniżej (podane wielkości są wielkościami minimalnymi):

	Parametry podstawowe	Ilość
1	Serwer www	
	CPU architektura: x86-64 2.4 GHz	4 vCPU
	RAM	8 GB
	HDD NVMe SSD	100 GB
2a	Serwer DEV aplikacji	
	CPU architektura: x86-64 2.4 GHz	4vCPU
	RAM	8 GB
	HDD NVMe SSD	200 GB
	Ipv4 adres zewnętrzny	1
	vLAN sieć wewnętrzna	1
2b	Serwer PROD aplikacji	
	CPU architektura: x86-64 2.4 GHz	4vCPU
	RAM	8 GB
	HDD NVMe SSD	200 GB
	Veeam Backup & Replication Standard for VMware lub równoważny	1
	HDD NVMe SSD	200 GB
	IPv4 adres zewnętrzny	1
	vLAN sieć wewnętrzna	1
3	Serwer Insert	
	CPU architektura: x86-64 2.4 GHz	4vCPU
	RAM	16 GB
	HDD NVMe SSD	200 GB
	Veeam Backup & Replication Standard for VMware lub równoważny	1
	HDD NVMe SSD	200 GB
	IPv4 adres zewnętrzny	1
	vLAN sieć wewnętrzna	1
4	Usługi dodatkowe	
	Microsoft® Exchange Standard 15 GB (Outlook) – Skrzynka pocztowa osobowa przypisana do konkretnej osoby	29
	Microsoft® Exchange Standard 15 GB (Outlook) – Skrzynka pocztowa techniczna	5
	Bitdefender antywirus serwera poczty Exchange lub równoważny	34
	Bitdefender antywirus stanowiska pracy lub równoważny	29
	Veeam Agent lub równoważny	29
	HDD NVMe SSD (240GBx29 User)	7000 GB
5	Wsparcie informatyczne	
	Wsparcie administratora w zakresie zarządzania infrastrukturą informatyczną lokalną oraz serwerową do poziomu OS, w tym w razie potrzeby, co najmniej 2 godz. w tygodniu w siedzibie Zamawiającego	28h/miesiąc
	Utrzymanie usługi Active Directory	1

- 7) Wykonawca zagwarantuje świadczenie Usługi na poziomie co najmniej opisanym poniżej, dla ośrodka przetwarzania danych, w ramach którego infrastruktury oferowane będą Usługi:
- a) teren ogrodzony, obiekt posiadający następujące zabezpieczenia: system telewizji przemysłowej (CCTV) z okresem archiwizacji min. 7 dni (monitorowane wszystkie wejścia do obiektu, monitorowane wszystkie pomieszczenia technologiczne, zapis obrazu z rejestracją aktualnej daty i godziny); system kontroli dostępu (z wyodrębnionym min. 3 poziomami dostępu); system sygnalizacji włamania i napadu; system wykrywania wody i zalania; ośrodek chroniony przez zewnętrzną licencjonowaną firmę;
 - b) ośrodek spełniający wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie: budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej;
 - c) ośrodek zlokalizowany na terenie Europejskiego Obszaru Gospodarczego na obszarze dla którego Komisja Europejska wydała decyzję uznającą odpowiedni stopień ochrony przetwarzania danych osobowych – wszystkie dane będą na tych obszarach przetwarzane (w tym w szczególności gromadzone i przechowywane);
 - d) ośrodek podłączony w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym;
 - e) węzeł telekomunikacyjny wyposażony w redundantny system firewall oraz system detekcji i prewencji włamań z sieci;
 - f) minimum dwie zewnętrzne linie zasilania;
 - g) system zasilania awaryjnego UPS osobno na każdą linię zasilającą + agregat prądotwórczy – system zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną, agregat prądotwórczy powinien posiadać zapas paliwa pozwalający na niezależną pracę bez konieczności uzupełnienia zbiorników przez co najmniej 8 godzin i musi umożliwiać uzupełnienie paliwa w trakcie jego pracy;
 - h) stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianych Zamawiającemu oraz przyjmowania zgłoszeń awarii;
 - i) Wykonawca spełnia wskazane poniżej normy potwierdzające działanie Wykonawcy w sposób gwarantujący zachowanie ciągłości działania na poziomie wymaganym przez Zamawiającego oraz bezpieczeństwo danych na poziomie wymaganym przez Zamawiającego i przepisy prawa:
 - ciągłości działania ISO 22301 na usługi IaaS i backup,
 - bezpieczeństwa informacji ISO 27001 na usługi IaaS i backup,
 - bezpieczeństwa informacji w chmurze ISO 27017 na usługi IaaS i backup,lub standardów lub norm równoważnych.
- 8) Wykonawca na każdorazowe wezwanie Zamawiającego w trybie następnego dnia roboczego zobowiązuje się dostarczyć Usługi Dodatkowe wymienione w pkt 3. ppkt 6) Usługi pozostałe ponad ilości wskazane w ramach opisu Usługi na poziomie parametrów podstawowych, ale nie przekraczające ilości wskazanej w ramach opisu Prawa opcji.
- 9) Zamawiający dopuszcza możliwość zaoferowania sprzętu (urządzeń), systemów (oprogramowania) o równoważnych lub lepszych parametrach technicznych od wymienionych w pkt 6) opisu. W takim przypadku Wykonawca, który powołuje się na rozwiązania

równoważne do opisywanych przez Zamawiającego, jest zobowiązany wykazać, że oferowany przez niego sprzęt (urządzenia, systemy czy oprogramowania), spełniają wymagania określone przez Zamawiającego. Podstawową formą wykazania, że urządzenie czy oprogramowanie są równoważne lub charakteryzują się lepszymi parametrami, jest przedstawienie szczegółowej specyfikacji technicznej do złożonej oferty.

- 10) Jeśli Wykonawca zaoferuje w ofercie przeprowadzenie szkolenia z zakresu bezpieczeństwa (punktowane kryterium oceny ofert) to wówczas Wykonawca przeprowadzi przynajmniej test dla wszystkich pracowników Zamawiającego ze znajomości zasad bezpieczeństwa informatycznego w postaci rozesłania przynajmniej 2 maili (tzw. test typu Phishing) zawierających linki do stron Wykonawcy lub we wskazane przez Wykonawcę miejsce w chmurze, aby zweryfikować, ilu pracowników skorzystało z tych linków. Po przeprowadzonym teście, Wykonawca przedstawi Zamawiającemu raport z przeprowadzonego testu oraz przeprowadzi szkolenie dla wszystkich pracowników Zamawiającego z zasad bezpieczeństwa informatycznego, ze szczególnym nastawieniem na ataki typu Phishing na podstawie otrzymanych rezultatów oraz aktualnej wiedzy dotyczącej tego typu prób ataków.

4. Prawo opcji

4.1. Prawo opcji dotyczy świadczenia usług obejmujących:

- ochronę antywirusową zgodnie z parametrami w pkt. 3 ustęp 3) ppkt. p) OPZ – maksymalnie dodatkowo 32 nowych stacji roboczych,
- poczta email i pakiet aplikacji biurowych zgodnie z parametrami w pkt 3 ustęp 3) ppkt. p), q) OPZ – maksymalnie dodatkowo 32 nowych kont pocztowych,
- przedłużenia świadczenia usługi opisanej w pkt 3 OPZ – maksymalnie do 28.02.2025 r., tj. o dwa miesiące kalendarzowe w stosunku do zakresu podstawowego (31.12.2024 r.).

4.2. Zamawiającemu przysługuje prawo skorzystania z opcji, zgodnie z art. 441 ustawy PZP.

4.3. W przypadku skorzystania przez Zamawiającego z prawa opcji, Wykonawcy przysługiwać będzie wynagrodzenie z tytułu wykonania zamówienia objętego prawem opcji obliczone na podstawie ceny jednostkowej wskazanej przez Wykonawcę w Formularzu ofertowym oraz zakresu wykonanej przez Wykonawcę usługi w ramach prawa opcji.

4.4. W celu skorzystania z prawa opcji Zamawiający przekaże Wykonawcy w przypadku przedłużenia świadczenia usługi oświadczenie o zamiarze skorzystania z prawa opcji, w formie pisemnej w terminie nie krótszym niż 7 dni przed skorzystaniem z tego prawa, a w przypadku zwiększenia ilości stacji roboczych lub kont pocztowych, w formie pisemnej w sposób uzgodniony z Wykonawcą w terminie nie krótszym niż 3 dni przed skorzystaniem z tego prawa.

4.5. Zamawiający może skorzystać z prawa opcji wielokrotnie – do momentu wyczerpania maksymalnego zakresu opcji określonego w pkt 4.1.

4.6. Zlecenie wykonania zamówienia objętego prawem opcji nie będzie wymagało zawarcia odrębnej umowy z Wykonawcą.

4.7. Wykonawcy nie przysługuje żadne roszczenie w stosunku do Zamawiającego w przypadku, gdy Zamawiający nie skorzysta z prawa opcji. Realizacja zamówienia objętego opcją jest wyłącznie uprawnieniem Zamawiającego.

4.8. W zakresie realizacji zamówienia objętego prawem opcji zapisy umowy, jaka zostanie zawarta w wyniku rozstrzygnięcia przedmiotowego postępowania, stosuje się odpowiednio.

5. Zatrudnienie na podstawie stosunku pracy

- 5.1. Zamawiający wymaga zatrudnienia przez Wykonawcę, jak i podwykonawcę, na podstawie stosunku pracy osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. -

Kodeks pracy (t.j. Dz.U. z 2018 r. poz. 917 z późn. zm.), tj. osób wykonujących następujące czynności:

- 1) administrowanie urządzeniami sieciowymi,
 - 2) administrowanie serwerami w środowisku wirtualnym,
 - 3) administrowanie systemami operacyjnymi.
- 5.2. W celu potwierdzenia spełnienia wymogu zatrudnienia na podstawie stosunku pracy przez Wykonawcę/podwykonawcę osób wykonujących czynności opisane w pkt. 3, Wykonawca przedstawi przed przystąpieniem do realizacji zamówienia **pisemne oświadczenie Wykonawcy/podwykonawcy o zatrudnieniu na podstawie stosunku pracy tych osób**. Oświadczenie to powinno zawierać w szczególności: dokładne określenie podmiotu składającego oświadczenie, datę złożenia oświadczenia, imię i nazwisko osoby ze wskazaniem jakie czynności wykonuje osoba zatrudniona na podstawie stosunku pracy, rodzaju umowy o pracę oraz podpis osoby uprawnionej do złożenia oświadczenia w imieniu Wykonawcy/podwykonawcy. Nieprzedłożenie oświadczenia będzie traktowane jako niewykazanie spełnienia wymogu zatrudnienia na podstawie stosunku pracy.
- 5.3. Zamawiający może w każdym czasie przeprowadzić kontrolę spełnienia ww. obowiązku, występując do Wykonawcy o złożenie stosownego oświadczenia. Nieprzedłożenie oświadczenia będzie traktowane jako niewykazanie spełnienia wymogu zatrudnienia na podstawie stosunku pracy.
- 5.4. Sankcje z tytułu niespełnienia ww. wymagań zostały określone w załączniku do SWZ - "Wzór umowy".