Zamówienie publiczne nr 4/2020

Usługi informatyczne w zakresie przechowywania danych
Szczegółowy opis przedmiotu zamówienia

KOD CPV:

72317000-0 - Usługi przechowywania danych

I. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa na rzecz Zamawiającego usługi informatycznej polegającej na gromadzeniu i bezpiecznym przechowywaniu danych z wykorzystaniem technologii obiektowej spełniającej funkcjonalności WORM (Write Once, Read Many), wytwarzanych w ramach aplikacji użytkowanej przez Toruńskie Centrum Usług Wspólnych.

Wykonawca będzie oferował usługę w oparciu o infrastrukturę technologiczną ośrodka centrum przetwarzania danych zlokalizowanego na terytorium Unii Europejskiej lub Lichtensteinu, Islandii, Norwegii. Ponadto Wykonawca musi zapewnić łącza do sieci Internet, infrastrukturę teletechniczną wraz z niezbędnymi urządzeniami, oprogramowaniem i licencjami potrzebnymi do prawidłowego uruchomienia i działania usługi. Wykonawca musi zapewnić wsparcie usługi w trybie 24/7/365.

Szczegółowe wymagania dotyczące realizacji zamówienia zawarte zostały również w punktach od **VIII-X** niniejszego zapytania.

Wszelkie użyte w niniejszym zapytaniu i załącznikach do niego nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, wymagane certyfikaty itp., w tym nazwy handlowe, oznaczenia lub znaki towarowe, patenty, określenia pochodzenia, źródła lub szczególnego procesu charakteryzujące produkt lub usługę dostarczane przez konkretnego wykonawcę, a które mogły pojawić się w zapytaniu i załącznikach do niego, należy rozumieć każdorazowo jak opatrzone dopiskiem „lub równoważne".

II. Termin rozpoczęcia i świadczenia usługi

Od dnia zawarcia umowy, ale nie wcześniej niż od dnia 01.11.2020 roku do dnia 31.12.2021 roku.

III. Miejsce i termin składania ofert

Wykonawca może złożyć tylko jedną ofertę w jednej z podanych form: w sekretariacie TCUW, pl. św. Katarzyny 9, 87-100 Toruń, na adres e-mail sekretariat@tcuw.torun.pl lub przesłać na adres Toruńskie Centrum Usług Wspólnych, pl. św. Katarzyny 9, 87-100 Toruń. Oferty prosimy składać w terminie **do 20.10.2020 r. do godz. 12:00.**

IV. Sposób obliczania ceny

1. Wykonawca poda cenę netto i brutto oferty w Formularzu Ofertowym, sporządzonym według wzoru stanowiącego Załącznik Nr 1.
2. Cena ofertowa podana przez wykonawcę w Formularzu Oferty zostanie ustalona jako cena łączna na okres ważności umowy i nie będzie podlegała zmianom.
3. Ceny muszą być wyrażone w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
4. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia oraz wszelkie opłaty i podatki wynikające z obowiązujących

przepisów. Cena musi zawierać wszystkie koszty przygotowania i złożenia oferty oraz świadczenie usługi przez okres wskazany w przedmiocie zamówienia.

5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
6. Rozliczenia między zamawiającym a wykonawcą będą prowadzone w PLN.
7. Płatność za usługę będzie zrealizowana jednorazowo w terminie do dnia 31.12.2020 roku.

V . Badanie ofert

1. Niespełnienie lub niewykazanie spełnienia któregokolwiek warunku lub braku podstaw do wykluczenia będzie przyczyną wykluczenia Wykonawcy i uznania jego oferty za odrzuconą. Zamawiający odrzuci również oferty, których treść nie będzie odpowiadać niniejszemu Szczegółowemu Opisowi Przedmiotowi Zamówienia.
2. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert. Zamawiający zastrzega możliwość weryfikacji i wizytacji wskazanego w ofercie ośrodka centrum przetwarzania danych, w tym złożenia dowodów dotyczących spełnienia wskazanych w zapytaniu wymagań.
3. Zamawiający w celu ustalenia, czy oferta zawiera rażąco niską cenę lub części składowe ceny wydają się rażąco niskie w stosunku do przedmiotu zamówienia, zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Zamawiający zwraca się o wyjaśnienia w szczególności w przypadku gdy cena całkowita oferty jest niższa o co najmniej 30% od:
   a) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub średniej arytmetycznej cen wszystkich złożonych ofert, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia.
   b) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu postępowania, w szczególności istotnej zmiany cen rynkowych.

   Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy. Zamawiający odrzuca ofertę wykonawcy, który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
4. Zamawiający poprawi w ofercie:
   a) oczywiste omyłki pisarskie,
   b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   c) inne omyłki polegające na niezgodności oferty z zapytaniem ofertowym, niepowodujące istotnych zmian w treści oferty,

   niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
5. Zamawiający zastrzega sobie, że może najpierw dokonać oceny ofert, a następnie zbadać, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
6. Zamawiający oceni i porówna jedynie te oferty, które nie zostaną wykluczone i odrzucone.
7. Postępowanie zostanie rozstrzygnięte w przypadku złożenia co najmniej jednej oferty niepodlegającej odrzuceniu.

VI. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty i sposobu oceny.

1. Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert:

Lp.	Nazwa kryterium	Waga kryterium (w %)
1	Cena brutto za całość usługi	60
2	Ośrodek przetwarzania danych	30
3	Dostępność usługi – SLA	10

2. Zamawiający dokona oceny ofert, przyznając punkty w ramach kryterium „Cena brutto za całość usługi" przyjmując zasadę, że 1% = 1 punkt.
3. Punkty za kryterium **„Cena netto za całość usługi"** zostaną obliczone według wzoru:

$$\frac{\text{cena oferty najtańszej}}{\text{cena oferty badanej}} \times 60 = LP$$

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

gdzie

LP = liczba uzyskanych punktów

4. Punkty za kryterium „**Ośrodek przetwarzania danych**" zostaną przyznane w skali punktowej od 0 do 30 pkt, wg poniższej zasady:
   a. Posiadany aktualny certyfikat ISO 27001 na usługi cloud computing: 5 pkt
   b. Posiadany aktualny certyfikat ISO 27017 na usługi cloud computing: 5 pkt
   c. Posiadany aktualny certyfikat ISO 22301 na usługi cloud computing: 5 pkt
   d. Posiadany aktualny certyfikat ANSI-TIA RATED 3: 5 pkt
   e. Posiadany certyfikat TIER III dokumentacji centrum przetwarzania danych: 5 pkt
   f. Posiadany certyfikat TIER III infrastruktury centrum przetwarzania danych: 5 pkt
5. Punkty za kryterium „**Dostępność usługi – SLA**" zostaną przyznane w skali punktowej do 10 pkt. wg poniższej zasady ramach:
   a. Gwarancja dostępności usługi od 99,95% a poniżej 99,99% SLA w skali roku – 0 pkt
   b. Gwarancja dostępności usługi 99,99% i więcej SLA w skali roku – 10 pkt
6. Liczby punktów, o których mowa w pkt 3 do 5 po zsumowaniu stanowić będą końcową ocenę oferty.
7. Za najkorzystniejszą zostanie uznana oferta z największą liczbą punktów, tj. przedstawiająca najkorzystniejszy bilans kryteriów oceny ofert.
8. Zamawiający nie dopuszcza składania ofert wariantowych ani częściowych.

9. Zamawiający oczekuje dołączenia do oferty poświadczonych za zgodność z oryginałem kopii aktualnych certyfikatów.

VII. Warunki udziału w postępowaniu

1. Wykonawca musi być zarejestrowanym operatorem telekomunikacyjnym nie krócej niż 3 lata od dnia złożenia oferty. Warunek zostanie oceniony na podstawie złożonych dokumentów w postaci potwierdzenia wpisu do właściwego rejestru.

2. Wykonawca musi dysponować ośrodkiem przetwarzania danych, spełniającym wymagania określone w części VIII. Warunek zostanie oceniony na podstawie oświadczenia Wykonawcy, złożonego zgodnie z pkt. 3 formularza oferty:

VIII. Wymagania dla ośrodka przetwarzania danych w ramach którego oferowana będzie usługa i Wykonawca będzie przetwarzał dokumenty Zamawiającego.

Wykonawca będzie realizować usługę z wykorzystaniem infrastruktury ośrodka przetwarzania danych spełniającego poniższe wymagania:

1. Wymagania obligatoryjne dla ośrodka.

OBIEKT I LOKALIZACJA		
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Lichtensteinu , Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Lichtensteinu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury.
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej.	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko).
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.
7	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).

8	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych.
9	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.
10	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.
11	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1.	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.
12	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.
WĘZŁY TELEKOMUNIKACYJNE		
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora.
2	Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
3	Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.
4	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.
5	Węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.
6	Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.
ZASILANIE		
1	Dostępność roczna systemu zasilania 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.

3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą .	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.
4	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.
5	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.	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.
6	Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.
BEZPIECZEŃSTWO		
1	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD).	Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń.
2	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.
3	Ochrona przez zewnętrzną licencjonowaną firmę.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.
4	System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.
5	System SKD dzieli centrum przetwarzania danych wraz z terenem przynależnym na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku.
7	Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
8	Dostęp do strefy II (część biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
9	Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.

	identyfikacyjnej współpracującej z SKD.	
10	Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
11	System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
12	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.
MONITOROWANIE		
	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.
	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.

2. Wymagania obligatoryjne. Ośrodek centrum przetwarzania danych musi posiadać zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Bezpieczeństwo sprzętu informatycznego:

	Zakres
1	Izolacja sprzętu krytycznego
2	Ochrona przed uszkodzeniem
3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego
4	Ochrona przed dostępem dla osób nieupoważnionych

3. Wymagania obligatoryjne. Naprawa i konserwacja sprzętu:

	Zakres
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.
3	Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy.
4	Ochrona przed dostępem dla osób nieupoważnionych.
5	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).
6	Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania.

7	Należy prowadzić rejestr incydentów, awarii i usterek.
8	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.

IX. Wymagania SLA i czas reakcji

a. SLA dla świadczonej usługi musi wynosić minimum 99,95% w skali roku.

b. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w systemie online Wykonawcy, który umożliwia podgląd wszystkich zgłoszeń, czas ich realizacji oraz bieżący status. Dostęp do systemu odbywa się za pomocą indywidualnego konta użytkownika utworzonego dla Zamawiającego.

c. Czas reakcji na zgłoszenie musi wynosić do 1h od przyjęcia zgłoszenia.

d. Czas realizacji zgłoszenia musi wynosić do 4h od przyjęcia zgłoszenia.

X. Specyfikacja usługi - minimalne wymagania

1. W ramach realizacji oferty Wykonawca musi dostarczyć usługę gromadzenia i bezpiecznego przechowywania danych w przestrzeni dyskowej z wykorzystaniem technologii obiektowej spełniającej jednocześnie funkcjonalności technologii WORM (Write Once, Read Many).
2. Usługa z funkcjonalnością technologii WORM musi zapewniać niezmienność i nieusuwalność danych przez zadany czas, zapewniający funkcjonalność trwałego nośnika informacji, tj. zgodnych z ustawą z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2020r. poz. 794ze zm.), ustawą z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2020 r. poz. 287 ze zm.), ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz164 ze zm.) oraz dyrektywą MiFID – Dyrektywa Parlamentu Europejskiego i Rady Europy 2004/39 WE z 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych i Dyrektywą Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniającą Dyrektywę 2011/61/WE (zwana „Dyrektywą MiFID II" lub „MiFID II") i dyrektywą PSD – Dyrektywą Parlamenty Europejskiego i Rady Europy 2007/64/WE z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego.
3. Usługa musi gwarantować dostęp do przestrzeni dyskowej dla łącznej ilości 300 000 (trzystu tysięcy) dokumentów. Zamawiający przewiduje, iż całkowity rozmiar pojedynczego dokumentu, który zostanie przesłany do przestrzeni dyskowej wynosi do 2 MB.
4. Usługa musi zostać dostarczona w ramach klastra wysokiej dostępności HA (High Availability). Dane składowane mają być minimum w dwóch kopiach na odseparowanych fizycznie i logicznie nośnikach w dwóch lokalizacjach/strefach. Każda kopia ma być niezależnie zabezpieczona przed utratą spowodowaną fizyczną awarią co najmniej dwóch dowolnych nośników danych (dysków), oraz fizycznego jednoczesnego uszkodzenia co najmniej dwóch serwerów kontrolujących pracę dysków. Zabezpieczenie każdej z dwóch stref musi zapewniać niezależną automatyczną odbudowę poziomu bezpieczeństwa w przypadku awarii dysku w czasie krótszym niż 1h. W przypadku awarii całego serwera czas automatycznego powrotu do pełnego poziomu bezpieczeństwa ma być krótszy niż 4h.
5. Usługa ma posiadać wbudowane mechanizmy przechowywania zarówno danych składowych jako obiekty, jak i metadanych systemowych oraz metadanych własnych (informacji opisujących obiekty / dane).
6. Usługa ma posiadać możliwość integrowania rozwiązania z istniejącym oprogramowaniem u Zamawiającego. Wymagane jest zapewnienie dostępu do danych poprzez REST API (REST – Representational State Transfer – styl architektury oprogramowania opierający się o zbiór wcześniej określonych reguł opisujących jak definiowane są zasoby, a także umożliwiających dostęp do nich. Preferowany format komunikatów to JSON), (API – Application Programming Interface – zestaw reguł definiujący komunikację pomiędzy programami komputerowymi).

7. Usługa ma posiadać funkcjonalność replikacji synchronicznej pomiędzy minimum dwoma przestrzeniami dyskowymi tego samego typu. Dane po replikacji mają w dalszym ciągu zachowywać cechy trwałego nośnika WORM.
8. Usługa ma posiadać wbudowane mechanizmy zapewniające możliwość potwierdzenia autentyczności danych składowanych. Mechanizmy te muszą opierać się o wyliczenia sumy kontrolnej dla każdego składowanego obiektu. Wymagane jest wsparcie dla co najmniej następujących algorytmów kryptograficznych: MD5, SHA-1, SHA-256, SHA-512.
9. Gwarancja dostępności danych cyfrowych zapisanych w przestrzeni dyskowej WORM ma obejmować okres 60 (sześćdziesięciu) miesięcy od daty zakończenia umowy. Po zakończeniu umowy, Gwarancja dostępności danych cyfrowych zapewnia udostępnienie dokumentów Zamawiającemu na jego wezwanie, przesłane na adres e-mail wskazany przez Wykonawcę, w terminie 14 dni od dnia wysłania wezwania.
10. Usługa ma posiadać mechanizm lub procedurę nieodwracalnego niszczenia danych, dla których okres retencji 60 miesięcy od dnia zakończenia umowy został przekroczony.

DYREKTOR
TORUŃSKIEGO CENTRUM USŁUG WSPÓLNYCH
Łukasz Nowak (5)

Zamówienie publiczne 4/2020

Załącznik nr 1. Formularz ofertowy

1. Informacje o Wykonawcy

Nazwa Wykonawcy	
Adres siedziby	
NIP	
Osoba do kontaktu	
Nr telefonu	
Adres e-mail	

2. Informacje o ofercie

Opis przedmiotu zamówienia/zakres oferty	
Całkowita cena netto usługi w PLN	
Całkowita cena brutto usługi w PLN	

3. Informacja o spełnieniu warunków udziału w postępowaniu - wymagania dla ośrodka w ramach którego oferowana będzie usługa i w którym wykonawca będzie przetwarzał dokumenty Zamawiającego.

1) Wykonawca jest zarejestrowanym operatorem telekomunikacyjnym nie krócej niż 3 lata od dnia złożenia oferty TAK/NIE* *(*zaznaczyć właściwe).*
2) Wymagania obligatoryjne dla ośrodka.

Wykonawca spełnia (TAK / NIE)

OBIEKT I LOKALIZACJA			
L.p.	Parametry lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Centrum przetwarzania danych zlokalizowane na terenie UE lub Lichtensteinu , Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.	

	Lichtensteinu, Islandii, Norwegii.		
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury.	
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej.	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.	
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko).	
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.	
7	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
8	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych.	
9	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu.	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	
10	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
11	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.	

	odporności włamaniowej zgodnie z EN 1143-1.		
12	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej.	
	WĘZŁY TELEKOMUNIKACYJNE		
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym.	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora.	
2	Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.	
3	Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP.	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.	
4	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.	
5	Węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.	
6	Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.	
	ZASILANIE		
1	Dostępność roczna systemu zasilania 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.	
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT.	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.	
3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą .	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.	
4	Redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.	
5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy	

	przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną.	urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.	
6	Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.	
	BEZPIECZEŃSTWO		
1	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD).	Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń.	
2	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.	
3	Ochrona przez zewnętrzną licencjonowaną firmę.	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.	
4	System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.	
5	System SKD dzieli centrum przetwarzania danych wraz z terenem przynależnym na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku.	
7	Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
8	Dostęp do strefy II (część biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	

9	Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
10	Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
11	System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
12	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.	
MONITOROWANIE			
	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7.	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.	

3) Wymagania obligatoryjne. Ośrodek centrum przetwarzania danych posiada zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Bezpieczeństwo sprzętu informatycznego:

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Izolacja sprzętu krytycznego	
2	Ochrona przed uszkodzeniem	
3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego	
4	Ochrona przed dostępem dla osób nieupoważnionych	

4) Wymagania obligatoryjne. Naprawa i konserwacja sprzętu:

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.	
3	Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy.	
4	Ochrona przed dostępem dla osób nieupoważnionych.	
5	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).	
6	Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania.	
7	Należy prowadzić rejestr incydentów, awarii i usterek.	
8	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	

4. Lokalizacja (adres) centrum przetwarzania danych:

_____

5. Posiadane certyfikaty:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

6. Gwarantowana oferowana „Dostępność usługi – SLA w skali roku" wyrażona w %

_____

7. Załącznik wymagane do formularza ofertowego:

1) Kopie certyfikatów wymienionych w pkt. 5 (potwierdzone za zgodność z oryginałem).
2) Potwierdzenie wpisu do rejestru przedsiębiorców telekomunikacyjnych

Załącznik nr 2. Wzór umowy

UMOWA nr .....

Nr _____

zawarta w Toruniu, w dniu _____ r. pomiędzy:

_____, reprezentowany przez:

_____ - _____

_____ - _____

zwaną dalej **Wykonawcą,**

a

_____, reprezentowany przez:

_____ - _____

_____ - _____

zwanym dalej **Zamawiającym,**

zwane dalej **Stronami.**

§1
Przedmiot Umowy

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego usługi informatycznej polegającej na gromadzeniu i bezpiecznym przechowywaniu danych z wykorzystaniem technologii obiektowej spełniającej funkcjonalności WORM (Write Once, Read Many – Zapisz raz, odczytuj wiele razy), wytwarzanych w ramach aplikacji użytkowanej przez Zamawiającego, zwanej dalej **Usługą**, na potrzeby przechowywania łącznej ilości 300.000 szt. elektronicznych dokumentów logicznych. Szczegółowy zakres Usługi został zawarty w zapytaniu ofertowym nr ..... i ofercie Wykonawcy z dnia .....
2. W Umowie następujące pojęcia i skróty będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z wielkiej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:
    1) Trwałe Usunięcie oznacza usunięcie informacji zapisanych na nosikach danych oraz wszelkich ich kopii w sposób uniemożliwiający jakiekolwiek ich odtworzenie.
    2) System Pamięci Obiektowej oznacza dowolny system pamięci trwałej reprezentowany w sposób obiektowy.
    3) Usługa WORM (Write Once, Read Many) oznacza usługę typu „Zapisz raz, odczytuj wiele razy" świadczoną z infrastruktury centrum przetwarzania danych zlokalizowanego w _____, przy ul. _____, za pomocą dostarczonych interfejsów API, z którymi Zamawiający integruje Aplikację Obsługująca Dokumenty.
    4) Aplikacja Obsługująca Dokumenty oznacza oprogramowanie zewnętrznego dostawcy używane przez Zamawiającego, które Zamawiający integruje z interfejsami Application Programming Interface (API) usługi WORM.
3. Usługa realizowana jest w sposób zapobiegający przypadkowemu lub celowemu usunięciu danych przez pojedyncze osoby, a także zapobiegający zmianie poufnych informacji, zgodnie z zastosowaną technologią WORM.
4. Szczegółowy zakres Usługi obejmuje oddanie do dyspozycji Zamawiającego zasobów informatycznych w modelu usługowym, w postaci przestrzeni dyskowej zaprojektowanej z funkcją jednokrotnego zapisu danych, bez późniejszej możliwości ich modyfikowania.

5. Usługa realizowana jest wraz z mechanizmami bezpieczeństwa, które uniemożliwiają przypadkowe lub celowe usunięcie danych.
6. Usługa realizowana jest w celu przechowywania danych w postaci elektronicznych pojedynczych dokumentów logicznych. Każdy z pojedynczych dokumentów logicznych zawiera własne dokumenty towarzyszące.
7. Usługa posiada mechanizmy definiowalnego i definitywnego usunięcia danych, umożliwiające praktyczną implementację prawa do zapomnienia, pozostające w zgodzie z wymogami 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).
8. Wykonawca udostępni Usługę od dnia zawarcia umowy, nie wcześniej niż od dnia 01.11.2020 r.

§2
Komunikacja

1. Wszelkie komunikaty, informacje i dokumentacje związaną z realizacją zawartej Umowy Strony będą przekazywały sobie drogą elektroniczną na adresy email wskazane poniżej, chyba że Strony postanowiły w treści Umowy inaczej.
   a) Wykonawca wyznacza adresy email: _____
   b) Zamawiający wyznacza adresy email: _____
2. Każda ze Stron zobowiązana jest do poinformowania drugiej Strony o zmianie danych kontaktowych, pod rygorem uznania komunikatów, zamówień, informacji i dokumentów przekazanych zgodnie z dotychczasowymi danymi za skutecznie doręczone.
3. Zmiana adresów email, o których mowa w ust. 1, powyżej nie wymaga aneksu do Umowy i odbywa się poprzez pisemne poinformowanie drugiej Strony.

§3
Wynagrodzenie

1. W zamian za świadczenie Usługi na zasadach określonych w niniejszej Umowie Zamawiający zobowiązuje się do zapłaty na rzecz Wykonawcy łącznego wynagrodzenia w wysokości brutto _____ złotych (słownie: _____). Jest to wynagrodzenie całkowite i maksymalne, które pozostanie niezmienne przez cały okres świadczenia Usługi.
2. Płatność zrealizowana zostanie w terminie do dnia: 31.12.2020 r.
3. Płatność Wynagrodzenia, o którym mowa w ust.1, nastąpi na podstawie prawidłowo wystawionej i doręczonej Zamawiającemu faktury Vat.
4. Zamawiający wyraża zgodę na otrzymanie faktury Vat drogą elektroniczną w formacie PDF, na adres email _____.
5. Za dzień dokonania zapłaty Strony uznają dzień, w którym zostanie obciążony rachunek bankowy Zamawiającego.

§4
Prawa i obowiązki Stron

1. Zamawiający na podstawie niniejszej Umowy otrzymuje możliwość korzystania z Usługi w okresie ustalonym w Umowie.
2. Zamawiający zobowiązany jest do korzystania z Usługi wyłącznie w sposób zgodny z obowiązującym prawem, postanowieniami Umowy, dobrymi obyczajami oraz charakterem i przeznaczeniem Usługi.
3. Zamawiający w szczególności nie może korzystać z Usługi w celu:

a. celowego powodowania przeciążenia, przepełniania, blokowania lub natłoku w sieci Internet, innych sieciach transmisji danych lub zasobach Wykonawcy;

b. naruszania praw osób trzecich, w szczególności dóbr osobistych, praw autorskich i innych praw własności intelektualnej.

4. Wykonawca zobowiązuje się do świadczenia Usługi będącej przedmiotem Umowy z najwyższą starannością. W szczególności zobowiązuje się zapewnić, aby Usługi były dostępne dla Zamawiającego w sposób ciągły, a elektroniczne dokumenty logiczne były należycie zabezpieczone w szczególności przed uszkodzeniem, utratą, ujawnieniem osobom nieuprawnionym.
5. Wykonawca zobowiązuje się do współpracy z Zamawiającym w celu dokonania integracji Usługi z posiadaną przez Zamawiającego Aplikacją Obsługującą Dokumenty. Zakres działań Wykonawcy zostaje ograniczony do dostarczenia Usługi wraz z interfejsami API, umożliwiającymi integracje zewnętrznych rozwiązań.
6. Wykonawca w ramach zapewnienia dostępności Usługi zobowiązuje się do utrzymywania prawidłowego działania i sprawności urządzeń i zasobów w ramach sieci Wykonawcy oraz prawidłowego działania Usługi.
7. Wykonawca zapewnia Zamawiającemu dostępność Usługi na poziomie SLA: .....% w skali roku podczas trwania Umowy.
8. Po zakończeniu Umowy Wykonawca zapewnia Zamawiającemu Gwarancję dostępności danych cyfrowych zapisanych w przestrzeni dyskowej WORM przez okres 60 (sześćdziesięciu) miesięcy, na każde jego wezwanie przesłane na adres e-mail Wykonawcy określony w §2, ust. 1 umowy , w terminie 14 dni od dnia wysłania wezwania. Strony wspólnie definiują, że po upływie Gwarancji dostępności danych cyfrowych każdy dokument logiczny zostanie Trwale Usunięty z przestrzeni dyskowej Wykonawcy
9. Wszelkie przerwy techniczne w dostępności Usługi niezbędne dla zapewnienia prawidłowości i ciągłości świadczenia Usługi zgodnie z umową, w szczególności w związku z obsługą, konserwacją, rozbudową lub aktualizacją zasobów sieci wewnętrznej Wykonawcy, uniemożliwiające lub ograniczające możliwość korzystania z Usług lub infrastruktury i danych informatycznych Zamawiającego, niezbędne dla prawidłowego świadczenia Usługi, nie mogą przekraczać 60 min jednorazowo i łącznie 120 minut w miesiącu. Planowe przerwy na prace techniczne nie są wliczane do czasu niedostępności usługi SLA. O planowanych przerwach na prace techniczne Wykonawca poinformuje Zamawiającego pocztą elektroniczną e-mail wraz z przewidywanym czasem zakończenia przerwy nie później niż na 48h przed planowaną przerwą.
10. Dostęp do urządzeń, systemów oraz oprogramowania w ramach świadczonej usługi uzyskiwać będą wyznaczeni pracownicy Wykonawcy oraz pracownicy serwisu zewnętrznego pod nadzorem Wykonawcy.
11. Wykonawca nie sprawdza, nie rozpowszechnia, ani też w żaden sposób nie wykorzystuje treści danych przechowywanych lub przesyłanych przez Zamawiającego, za wyjątkiem sprawdzania łącznej liczby wgranych dokumentów logicznych oraz ich rozmiaru.
12. Na każde żądanie Zamawiającego przesłanego na adres e-mail Wykonawcy określony w §2, ust. 1 umowy Wykonawca w terminie 7 dni od otrzymania żądania umożliwi Zamawiającemu pobrania kopii wszystkich dokumentów logicznych przechowywanych w ramach Umowy. Powyższe obowiązuje również w okresie Gwarancji dostępności danych cyfrowych.
13. W przypadku wypowiedzenia, rozwiązania lub wygaśnięcia Umowy przed końcem obowiązywania umowy określonym w §12 ust. 1 niniejszej umowy, Wykonawca w terminie 7 dni od otrzymania żądania przesłanego pisemnie lub na adres e-mail Wykonawcy określony w §2, ust. 1 umowy, wyda Zamawiającemu wszystkie przechowywane w ramach Umowy dokumenty logiczne. Po potwierdzeniu poprawności wykonanej kopii, lecz nie później niż 30 dni od dnia wydania Wykonawca Trwale Usunie te dokumenty z wszystkich swoich zasobów.
14. Zamawiający ma prawo do uruchomienia ciągłej kopii danych wraz z kopią Aplikacji Obsługującą Dokumenty przechowywanych w ramach Umowy w innym centrum przetwarzania danych.
15. Zamawiający ma prawo do uruchomienia innej usługi WORM wraz z Aplikacją Obsługującą w innym centrum przetwarzania danych, do którego następuje ciągła kopia danych opisana ust. 14.

16. Wykonawca obowiązany jest do samodzielnego wykonywania przedmiotu Umowy i nie jest uprawniony do powierzania jej realizacji innym podmiotom bez uprzedniej pisemnej (pod rygorem nieważności) zgody Zamawiającego.

§ 5
Odpowiedzialność Stron

1. Wykonawca ponosi na podstawie Umowy pełną odpowiedzialność odszkodowawczą wobec Zamawiającego za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy.
2. Zamawiający jest zobowiązany do należytego zabezpieczenia własnych danych dostępu do indywidualnych kont użytkowników udostępnionych przez Wykonawcę. Zamawiający ponosi odpowiedzialność za skutki wyłącznie świadomego udostępnienia danych dostępu osobom niepowołanym.
3. Wykonawca nie ponosi odpowiedzialności za ewentualne szkody spowodowane:
   a) okolicznościami wynikającymi z wyłącznej winy osób trzecich lub Zamawiającego, w szczególności naruszeniem przez Zamawiającego postanowień Umowy;
   b) działaniem nielegalnego oprogramowania zainstalowanego przez Zamawiającego;
   c) działaniem wirusów komputerowych lub złośliwym działaniem osób trzecich, jeżeli wykaże, że działając z najwyższą starannością, właściwą zawodowemu charakterowi świadczonych usług, nie był w stanie zapobiec ich zaistnieniu lub skutkom
4. W przypadku, gdy z tytułu niewykonania lub nienależytego wykonania przez Wykonawcę, z przyczyn leżących po jego stronie, zobowiązań wynikających z postanowień niniejszej Umowy, zostanie zasądzone prawomocnym wyrokiem sądu od Zamawiającego na rzecz jakiejkolwiek osoby trzeciej odszkodowanie, Wykonawca zobowiązuje się pokryć wszelkie straty poniesione przez Zamawiającego w związku zaspokojeniem roszczeń takiej osoby, w szczególności łącznie z odsetkami i kosztami sądowymi, w terminie 7 (siedmiu) dni roboczych od daty otrzymania wezwania do zapłaty od Zamawiającego.
5. Zamawiający niezwłocznie powiadomi Wykonawcę o zgłoszonym przeciwko Zamawiającemu roszczeniu, wynikającym ze zdarzeń, o których mowa w ust.4 powyżej, a Wykonawca bez zbędnej zwłoki przekaże Zamawiającemu pisemne stanowisko dotyczące zasadności zgłoszonego roszczenia. W przypadku postępowania sądowego Zamawiający podejmie stosowne czynności zmierzające do umożliwienia Wykonawcy wzięcia udziału w tym postępowaniu i na zasadach określonych w obowiązujących przepisach prawa.

§ 6
Prawa autorskie

1. Wykonawca oświadcza i zapewnia, iż posiada majątkowe prawa autorskie oraz odpowiednie licencje do korzystania z oprogramowania w celu świadczenia Usługi dla Zamawiającego.
2. O ile jest to konieczne dla prawidłowego świadczenia Usługi, Wykonawca udzieli Zamawiającemu niewyłącznej i nieprzenaszalnej licencji/sublicencji na korzystanie z oprogramowania, w zakresie niezbędnym do korzystania z Usług zgodnie z ich przeznaczeniem oraz korzystania z dokumentów zapisanych w ramach Usługi po zakończeniu jej świadczenia.

§ 7
Ochrona danych osobowych

1. Zamawiający może w związku z korzystaniem z Usługi przechowywać lub przeprowadzać operacje na danych osobowych..
2. Zamawiający jest Administratorem danych osobowych, o których mowa w ust. 1 powyżej lub ich procesorem. Wykonawca nie decyduje o celach i środkach przetwarzania tych danych osobowych, a jedynie udostępnia w ramach świadczenia Usługi zasoby pozwalające na przechowywanie danych. Wykonawca stosuje środki techniczne i organizacyjne zapewniające ochronę danych

przechowywanych i przetwarzanych przez Zamawiającego zgodnie z odpowiednimi, obowiązującymi przepisami o ochronie danych osobowych.

3. Wykonawca oświadcza, że serwery za pomocą których świadczone są Usługi będące przedmiotem Umowy znajdują się na terenie Unii Europejskiej a przechowywane dane w żadnym przypadku w toku świadczenia Usługi nie są przesyłane poza obszar Unii Europejskiej.
4. Wykonawca zobowiązuje się zawrzeć z Zamawiającym w zakresie niezbędnym dla prawidłowego świadczenia Usługi odrębną umowę o powierzeniu przetwarzania danych osobowych najpóźniej w dniu rozpoczęcia świadczenia Usługi będącej przedmiotem niniejszej Umowy, według wzoru obowiązującego u Zamawiającego.

§ 8
Wsparcie techniczne

1. Wykonawca zobowiązuje się do niezwłocznego usuwania awarii urządzeń w ramach swojej sieci wewnętrznej, za prawidłowe działanie których ponosi odpowiedzialność zgodnie z postanowieniami Umowy. Za awarię uważa się nieprawidłowe działanie urządzenia powodujące przerwę w świadczeniu Usługi, trwającą dłużej niż 30 minut.
2. Zamawiający zgłasza awarie lub zapotrzebowanie na wsparcie informatyczne za pomocą indywidualnego konta użytkownika w systemie dostępnym pod adresem www ..... lub pocztą elektroniczną wyłącznie z użyciem adresów email wskazanych w § 2 ust. 1 lit. a) i b).
3. Jeżeli w wyniku analizy zgłoszenia nie zostanie potwierdzone istnienie awarii lub jeśli ustalona przyczyna awarii nie wynika z okoliczności, za które odpowiedzialność ponosi Wykonawca, Wykonawca powiadomi Zamawiającego o braku podstaw do interwencji.
4. Jeżeli w wyniku analizy zgłoszenia zostanie ustalona przyczyna awarii mieszcząca się w zakresie odpowiedzialności Wykonawcy, Wykonawca niezwłocznie przystąpi do usuwania awarii.
5. Wykonawca zobowiązuje się do usuwania awarii w najwcześniejszym możliwym terminie w normalnym toku czynności, z uwzględnieniem charakteru i rozmiaru awarii. Czas reakcji Wykonawcy na zgłoszenie awarii wynosi maksymalnie do 1 godziny, a maksymalny czas na usunięcie awarii –maksymalnie 4 godziny od przyjęcia zgłoszenia.
6. W przypadku wymiany urządzeń Wykonawcy zawierających dokumenty logiczne Zamawiającego przechowywane w ramach Umowy, Wykonawca Trwale Usunie te dane logiczne z wymienianych urządzeń po ich przeniesieniu na nowe urządzenia.

§ 9
Ochrona Informacji Poufnych

1. Strony zobowiązują się do zachowania ścisłej poufności polegającej na tym, iż nie ujawnią żadnej nieuprawnionej osobie trzeciej Informacji Poufnych. Strony nie mogą wykorzystywać Informacji Poufnych inaczej niż do celów określonych w niniejszej Umowie. Uchylenie zobowiązania do zachowania poufności wymaga uprzedniej pisemnej zgody odpowiedniej Strony niniejszej Umowy.
2. Przez Informacje Poufne Strony rozumieją informacje lub materiały odnoszące się do działalności Strony Umowy oraz stosunków cywilnoprawnych łączących Strony z podmiotami trzecimi lub wzajemnie oraz informacje wynikające lub związane z takimi stosunkami a także wszelkie informacje dotyczące Stron i związane prowadzoną przez Strony z działalnością gospodarczą, informacje finansowe, techniczne, naukowe oraz informacje innego rodzaju, włączając w powyższe specyfikacje a także informacje dotyczące ich podmiotów zależnych lub podmiotów z nimi trwale powiązanych kontraktami, które zostały ujawnione przez jedną ze Stron („Stronę Ujawniającą") drugiej Stronie („Stronie Otrzymującej") w związku z wykonywaniem Umowy lub przekazane przez osobę trzecią będącą wykonawcą, działającą w imieniu Strony. Informacjami Poufnymi są dane, które posiadając wartość gospodarczą mogą być uznane za poufne lub zostały udostępnione drugiej z zastrzeżeniem poufności, niezależnie od formy ich udostępnienia w jakiejkolwiek formie oraz na jakimkolwiek nośniku, zarówno materialnym, jak i niematerialnym, w tym ustnie, na piśmie

lub drogą elektroniczną. Informacjami Poufnymi są również informacje, których obowiązek utrzymania w tajemnicy obciąża Stronę Umowy na zgodnie z obowiązującymi przepisami o ochronie danych osobowych..

3. Za Informacje Poufne w rozumieniu niniejszej Umowy uznaje się również treść danych przechowywanych lub przesyłanych przez Zamawiającego z wykorzystaniem zasobów Wykonawcy udostępnionych w związku ze świadczeniem usług będących przedmiotem Umowy.
4. Strona Otrzymująca zachowa Informacje Poufne Strony Ujawniającej w tajemnicy i w stosunku do nich podejmie co najmniej takie same środki ostrożności, oraz co najmniej takie same środki zabezpieczające, jak te stosowane przez Stronę Otrzymującą w stosunku do jej własnych Informacji Poufnych, gwarantując tym samym, że zapewniają one odpowiednią ochronę przeciwko nieupoważnionemu ujawnieniu, kopiowaniu lub wykorzystaniu. Strona Otrzymująca zapewni, że ujawnianie Informacji Poufnych ograniczone będzie do tych pracowników, członków władz Strony Otrzymującej, którym wiedza taka jest niezbędna dla realizacji Umowy i którzy będą poinformowani o obowiązkach Stron wynikających z Umowy, i zobowiązani do postępowania zgodnie z zasadami wynikającymi z Umowy. Strony nie będą wykonywać kopii Informacji Poufnych, chyba że będzie to konieczne w zakresie niezbędnym dla realizacji Umowy.. Wszelkie Informacje Poufne oraz ich kopie zostaną zwrócone Stronie Ujawniającej w ciągu trzydziestu dni od otrzymania pisemnego żądania od Strony Ujawniającej
5. Obowiązek zachowania poufności nie dotyczy Informacji Poufnych:
   a) których ujawnienia wymagają bezwzględnie obowiązujące przepisy prawa;
   b) których ujawnienie następuje na żądanie podmiotu uprawnionego do kontroli, pod warunkiem; że podmiot ten został poinformowany o poufnym charakterze informacji;
   c) które są lub staną się publicznie dostępne w jakikolwiek sposób bez naruszenia Umowy przez Stronę Otrzymującą;
   d) w których posiadanie Strona weszła zgodnie z obowiązującymi przepisami prawa, przed dniem uzyskania takich informacji na podstawie Umowy;
   e) dotyczących faktu zawarcia Umowy, z wyłączeniem jej postanowień szczególnych, w zakresie wykorzystania tej okoliczności w materiałach marketingowych Strony lub ewentualnie referencji i potwierdzenia posiadanych kompetencji;
   f) dotyczących faktu zawarcia Umowy oraz jej postanowień szczególnych, których ujawnienie następuje na żądanie podmiotu prowadzącego audyt lub świadczącego pomoc prawną pod warunkiem, że podmiot ten został poinformowany o poufnym charakterze informacji.
6. W wypadku, gdy Strona zostanie zobowiązana nakazem sądu bądź organu administracji państwowej do ujawnienia Informacji Poufnych albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie druga Stronę oraz poinformować odbiorcę Informacji Poufnych o ich poufnym charakterze.
7. Obowiązek zachowania poufności wiąże Strony w okresie obowiązywania Umowy jak również przez okres 2 lat po jej wygaśnięciu lub rozwiązaniu- dotyczy Zamawiającego, a bezterminowo, nie krócej niż przez 10 lat po jej wygaśnięciu lub rozwiązaniu w przypadku Wykonawcy.

§ 10
Kary umowne

1. W przypadku wystąpienia przerw w dostępności Usługi, których łączny czas spowoduje spadek dostępności Usługi poniżej gwarantowanego poziomu SLA, o którym mowa w §4 ust. 7 umowy, Zamawiający jest uprawniony do naliczenia kary umownej w wysokości 500,00 zł za każdy rozpoczęty 1% niedostępności Usługi poniżej gwarantowanego poziomu SLA, o którym mowa powyżej.
2. Maksymalna wysokość kar wynosi do 100% wartości wynagrodzenia, o którym mowa w §3 ust. 1 Umowy.

3. W przypadku wystąpienia okoliczności uzasadniających zapłatę przez Wykonawcę kar umownych, Zamawiający może według własnego wyboru:
   a) potrącać kary umowne z wynagrodzenia należnego Wykonawcy;
   b) wezwać Wykonawcę do zapłaty kar umownych w terminie 14 dni od daty otrzymania pisemnego wezwania do ich zapłaty.
4. Niezależnie od postanowień powyższych Zamawiający jest uprawniony do dochodzenia odszkodowania przewyższającego zastrzeżone kary umowne na zasadach ogólnych do wartości rzeczywiście poniesionej szkody z wyłączeniem utraconych korzyści.

§ 11
Ograniczenie, zawieszenie Usług, Reklamacje

1. Reklamacje Zamawiającego w związku z niewykonaniem lub nienależytym wykonaniem Usługi powinny być przesyłane w formie pisemnej lub na adres e-mail Wykonawcy określony w §2, ust. 1 umowy i określać:
   a) numer i datę zawarcia Umowy;
   b) nazwę Zamawiającego
   c) rodzaj Usługi i parametry techniczne;
   d) zarzuty Zamawiającego i okoliczności uzasadniające reklamację,
   e) ewentualny proponowany sposób rozstrzygnięcia reklamacji.
2. Wykonawca udzieli odpowiedzi na reklamację w terminie 14 dni roboczych od momentu jej otrzymania.
3. W odpowiedzi na reklamację Wykonawca wskaże czy uznaje reklamację oraz w jaki sposób zamierza ją rozpatrzyć oraz w jakim terminie lub poinformuje o braku podstaw do uznania reklamacji wraz z uzasadnieniem swojego stanowiska. Brak odpowiedzi Wykonawcy w terminie, o którym mowa w ust. 2 powyżej jest równoznaczny z uznaniem reklamacji.

§ 12
Okres obowiązywania Umowy

1. Niniejsza Umowa została zawarta na czas określony od dnia .....do dnia 31.12.2021 roku.
2. Wykonawca ma prawo do natychmiastowego zaprzestania świadczenia Usługi oraz do wypowiedzenia Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo zawiadomienia Zamawiającego o dostrzeżonych nieprawidłowościach i udzielenia odpowiedniego, nie krótszego niż 7 dni, terminu na ich usunięcia Zamawiający nadal narusza przepisy prawa lub istotne postanowienia Umowy;
3. Zamawiający ma prawo wypowiedzenia Umowy bez zachowania okresu wypowiedzenia, jeżeli pomimo zawiadomienia Wykonawcy o dostrzeżonych nieprawidłowościach i udzielenia odpowiedniego, nie krótszego niż 7 dni, terminu na ich usunięcie Wykonawca nadal narusza przepisy prawa lub istotne postanowienia Umowy.
4. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
5. W przypadku wypowiedzenia lub odstąpienia od umowy Wykonawca może żądać wynagrodzenia jedynie za część umowy wykonaną do dnia ustania obowiązywania umowy (wyliczonego proporcjonalnie do liczby dni świadczenia Usługi w stosunku do wszystkich dni, na które umowa była zawarta). Jeżeli Wykonawca otrzymał wcześniej (z góry) zapłatę całości wynagrodzenia za świadczenie Usług, wówczas zobowiązany jest do zwrotu pozostałej części otrzymanego wynagrodzenia w terminie 7 dni od dnia zakończenia obowiązywania umowy.
6. Oświadczenie o odstąpieniu, wypowiedzeniu lub rozwiązaniu Umowy powinno zostać złożone na piśmie pod rygorem nieważności.

§ 13

Postanowienia końcowe

1. Zmiany Umowy wymagają formy pisemnego aneksu pod rygorem nieważności.
2. Prawem właściwym dla zobowiązań wynikających z Umowy jest prawo polskie.
3. Wszelkie spory wynikające z Umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla Zamawiającego. Strony zobowiązują się w każdym przypadku dążyć do ugodowego rozstrzygnięcia sporu powstałego na gruncie stosowania niniejszej Umowy.
4. Wszelkie zawiadomienia i oświadczenia związane z Umową mogą być składane za pomocą poczty elektronicznej na adresy email wskazane w paragrafie §2, ust. 1, za wyjątkiem oświadczeń dla których Umowa wyraźnie wymaga formy pisemnej. Oświadczenia w formie pisemnej przesyłane będą na adresy Stron podane na wstępie Umowy.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. **Zapytanie ofertowe nr ..... z dnia ..... i oferta Wykonawcy z dnia ....., stanowią załączniki nr ..... i ..... do niniejszej umowy i stanowią jej integralną część.**

Wykonawca	**Zamawiający**