Załącznik nr 9a
do warunków technicznych

INSTRUKCJA
PRZYGOTOWANIA ŚRODOWISKA DO PRACY TERMINALOWEJ WEGA

Niniejsza instrukcja zawiera opis instalacji komponentów niezbędnych do pracy terminalowej z systemem WEGA z lokalizacji zdalnej (poza siecią ZGiKM GEOPOZ). Kolejność wykonywania poszczególnych czynności ma znaczenie dlatego należy postępować zgodnie z wytycznymi. Praca zdalna odbywa się z zachowaniem poniższych zasad:

1) stacja robocza, z której dokonywane jest połączenie posiada system operacyjny Windows 10 lub nowszy (najlepiej w wersji 64 bitowej)
2) stacja robocza posiada podłączenie do Internetu
3) na stacji roboczej zainstalowane są komponenty wg niniejszej instrukcji (łącze VPN realizowane jest w oparciu o Palo Alto Global Protect a klient terminala w oparciu o VMware Horizon Client)
4) do stacji roboczej logują się tylko uprawnione osoby posiadające upoważnienie do przetwarzania danych osobowych zawartych w zbiorze „Ewidencja gruntów i budynków"
5) ze względów organizacyjnych i technicznych praca zdalna może być prowadzona w dniach roboczych w godzinach 8.00-20.00 przy czym w godzinach od 8.00-15.30 ZGiKM GEOPOZ zapewnia pomoc telefoniczną swoich pracowników
6) podczas pracy zdalnej stacja robocza jest automatycznie odcinana od sieci lokalnej użytkownika i możliwe jest korzystanie tylko z zasobów lokalnych stacji roboczej (dyski, drukarki) oraz zasobów zdalnych udostępnionych przez ZGiKM GEOPOZ
7) ZGiKM GEOPOZ nie odpowiada za jakość łączy internetowych (np. ich stabilność i przepustowość)

UWAGA!!!

Część A zawiera opis instalacji niezbędnych komponentów

Część B zawiera opis pierwszego uruchomienia tunelu VPN i terminala

Część C zawiera opis bieżącej pracy z tunelem VPN i terminalem

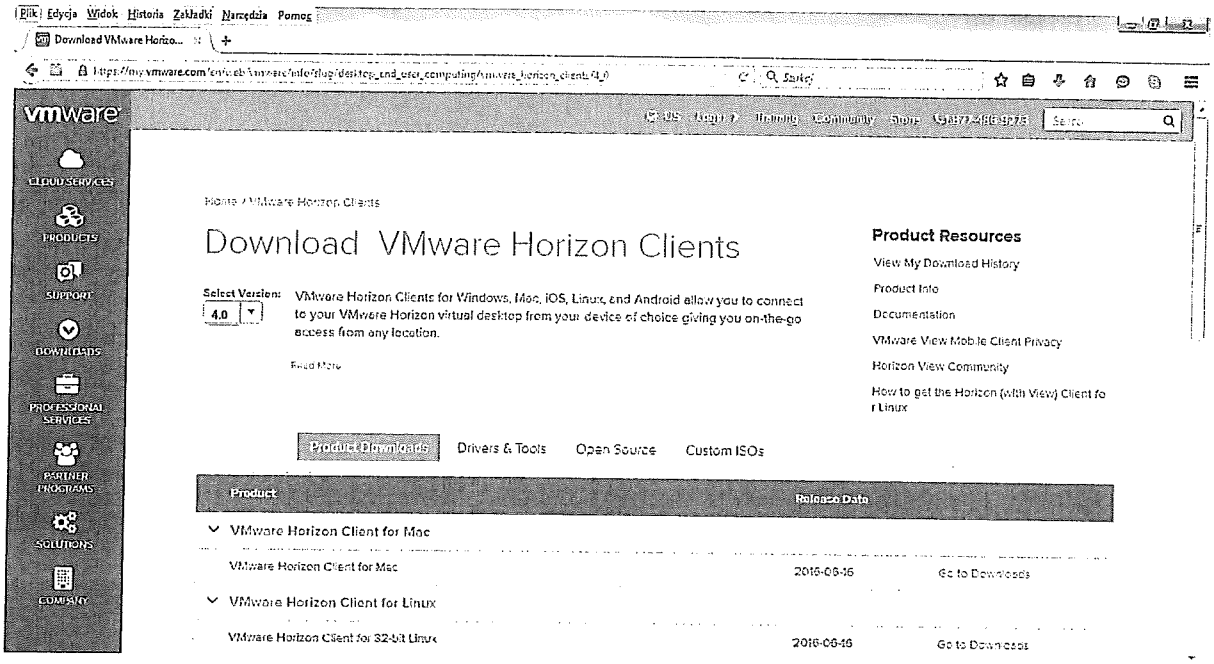
Część D zawiera opis udostępniania zasobów lokalnych stacji roboczej

Po wykonaniu czynności z części A i B, kolejne połączenia do terminala systemu WEGA wykonywane są tylko wg opisu z części C. Nie należy ponownie wykonywać czynności z części A i B.

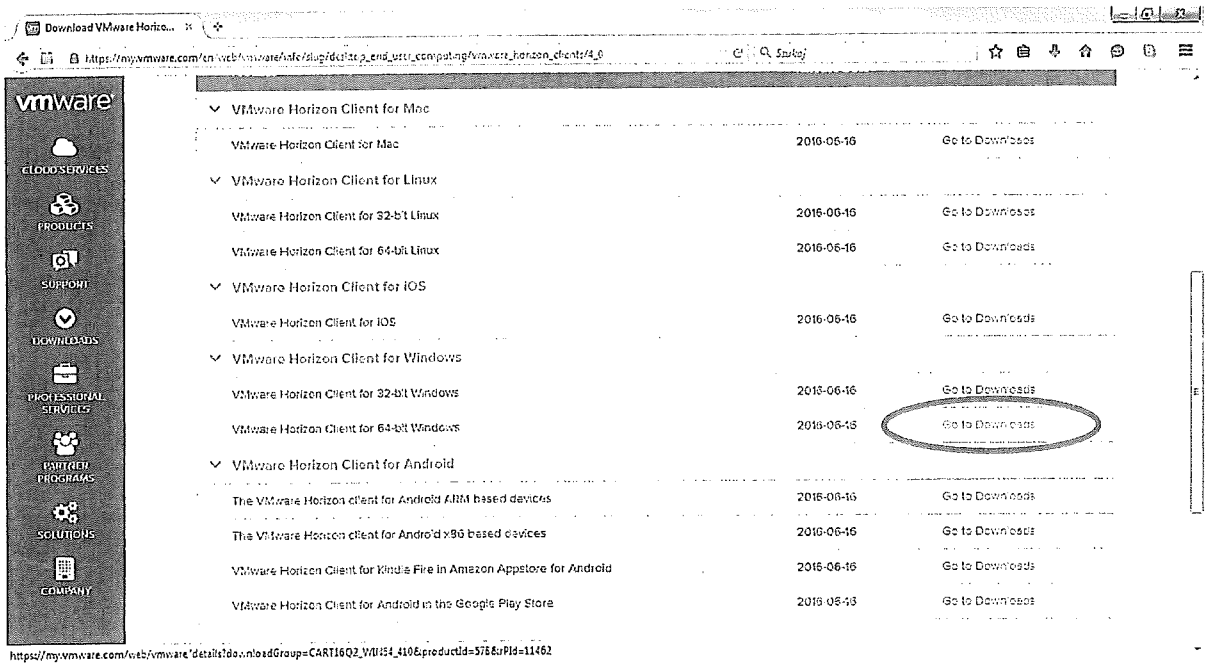
A. Instalacja komponentów

INSTALACJA KLIENTA TERMINALA

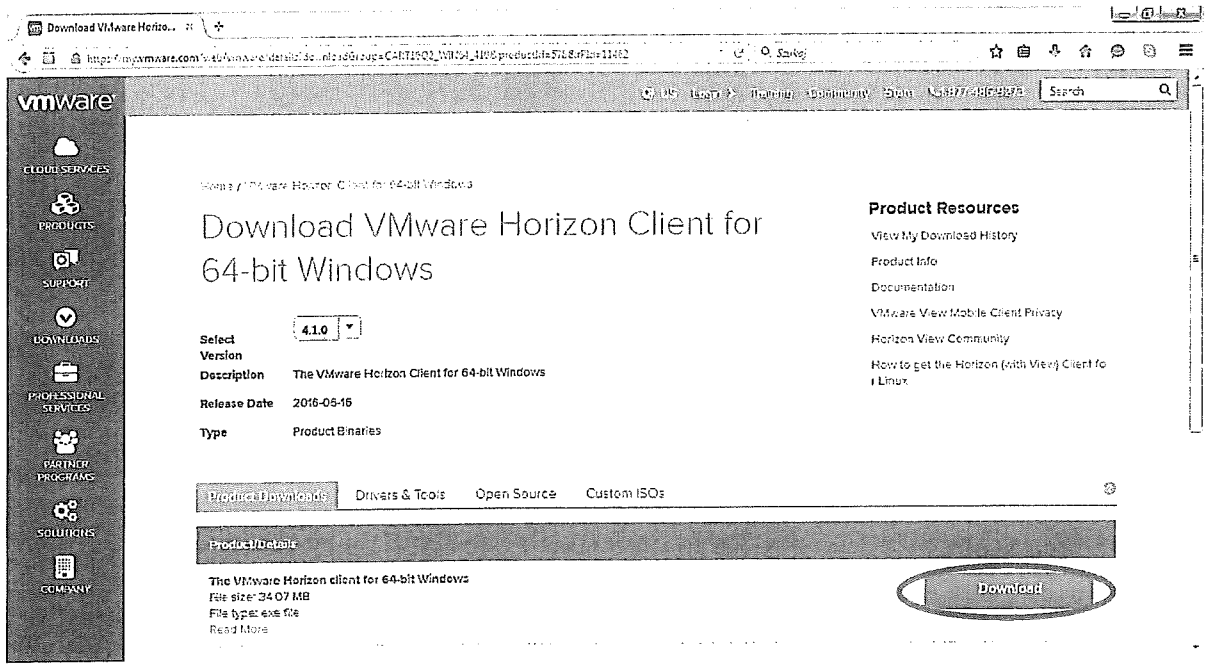
1. Uruchomić przeglądarkę i wpisać adres strony do pobrania klienta VMware (oprogramowanie bezpłatne, licencje posiada ZGiKM GEOPOZ) https://my.vmware.com/en/web/vmware/info/slug/desktop_end_user_computing/vmware_horizon_clients/4_0



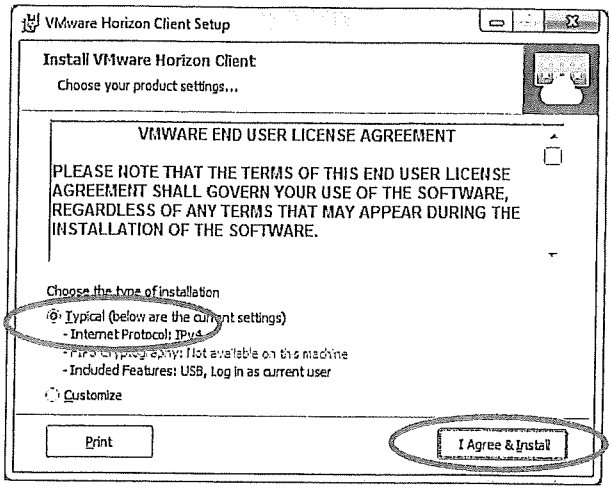
2. Wybrać klienta właściwego dla posiadanego systemu operacyjnego (np. zgodnie z zaleceniami dla Windows 10 64 bit)

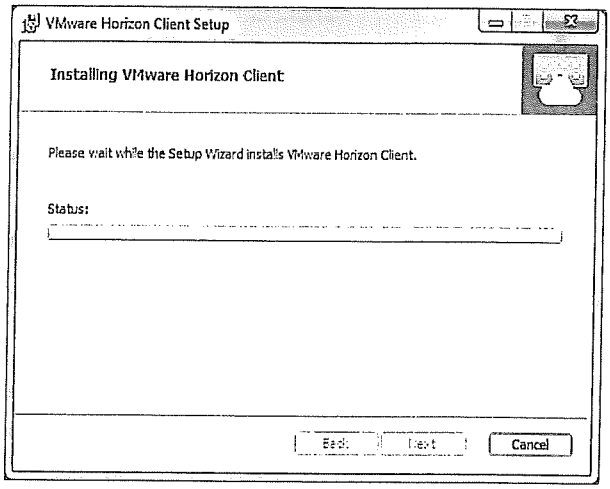


3. Pobrać wybranego klienta

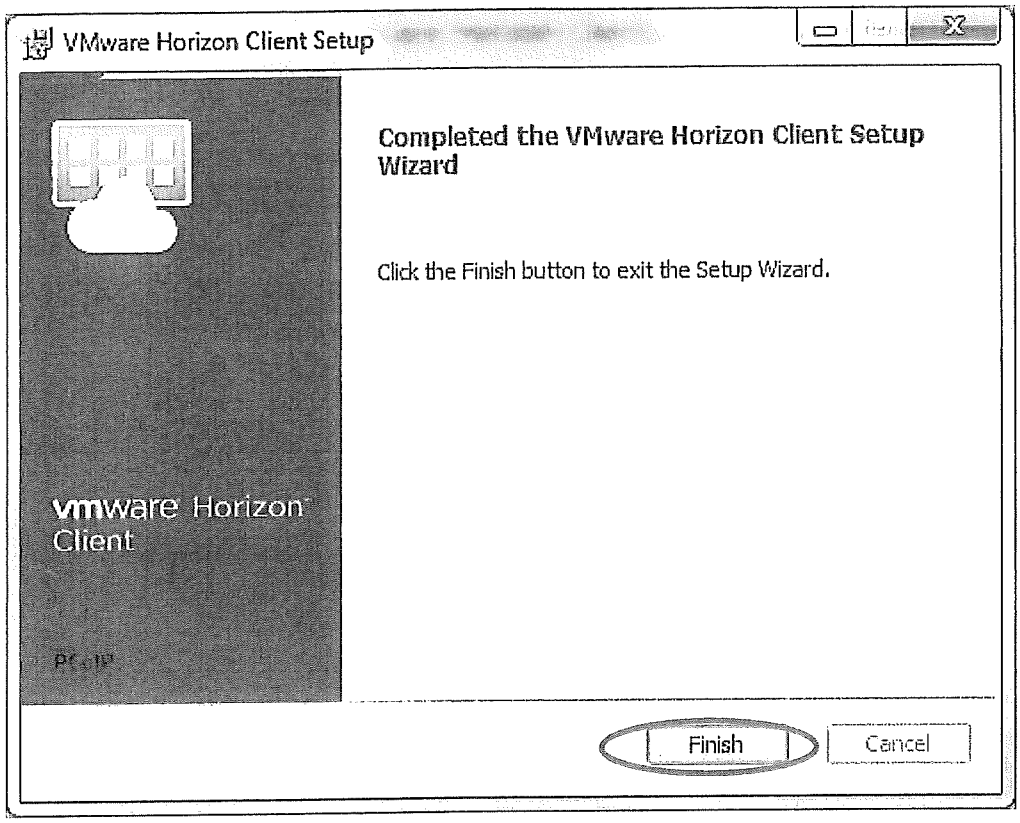


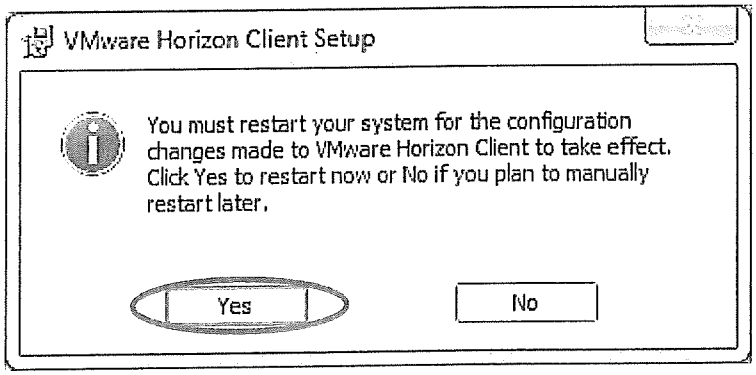
4. Zainstalować wybranego klienta wybierając opcję **Typical**



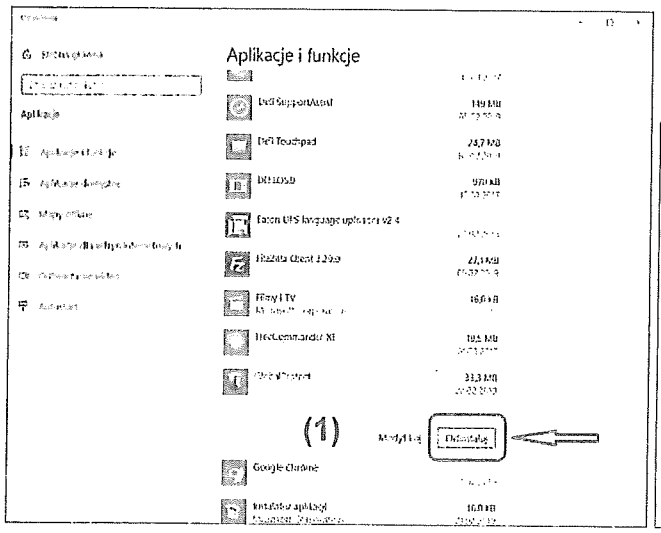


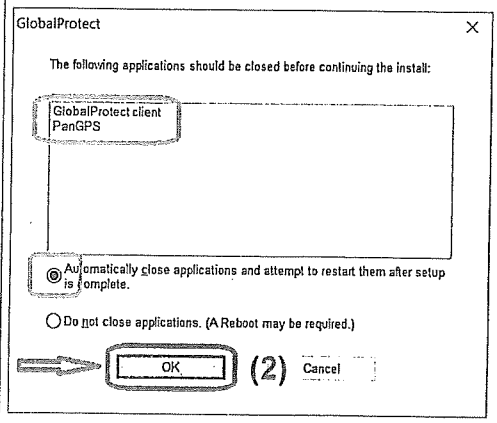
5. Po zakończeniu instalacji wykonać restart komputera


VMware Horizon Client Setup
Completed the VMware Horizon Client Setup Wizard
Click the Finish button to exit the Setup Wizard.
vmware Horizon Client
Finish
Cancel


VMware Horizon Client Setup
You must restart your system for the configuration changes made to VMware Horizon Client to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

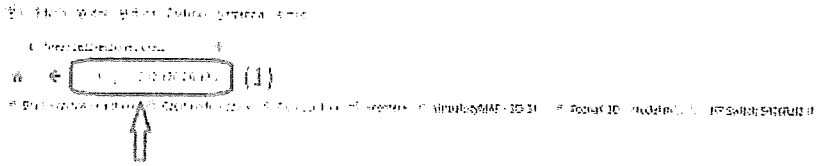
6. Przed instalacją nowej wersji klienta VPN należy sprawdzić czy na stacji jest zainstalowana wcześniejsza wersja i najpierw ją odinstalować.

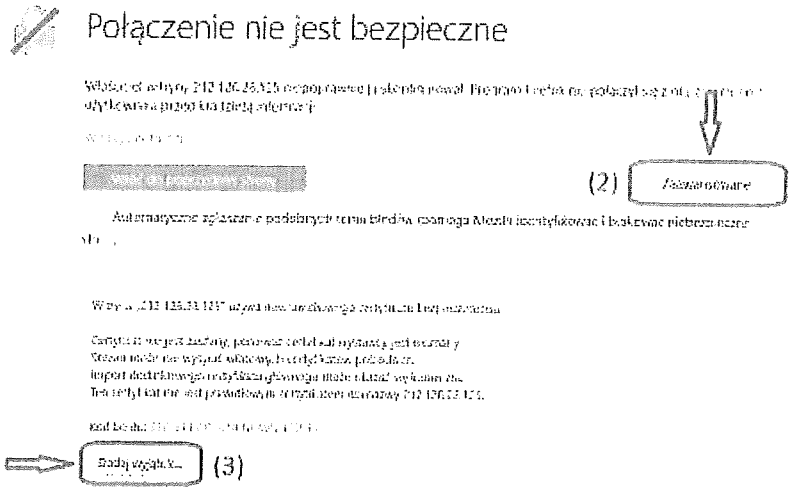




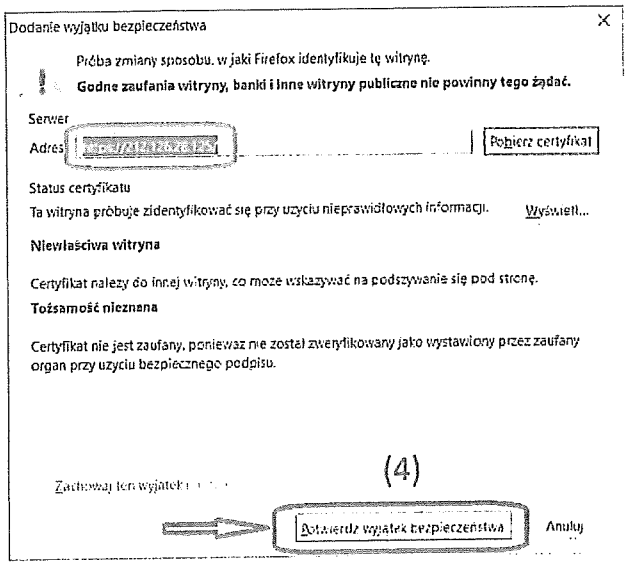
Po uruchomieniu procesu deinstalacji może pojawić się informacja o potrzebie zamknięcia działających aplikacji klienta Global Protect i wtedy należy wymusić ich zamknięcie przyciskiem OK.

7. Uruchomić przeglądarkę i wpisać adres strony do pobrania klienta VPN (oprogramowanie bezpłatne, licencje posiada ZGiKM GEOPOZ) https://212.126.28.125 (1) a po wyświetleniu strony kliknąć przycisk **Zaawansowane** (2), następnie przycisk **Dodaj wyjątek...**(3).

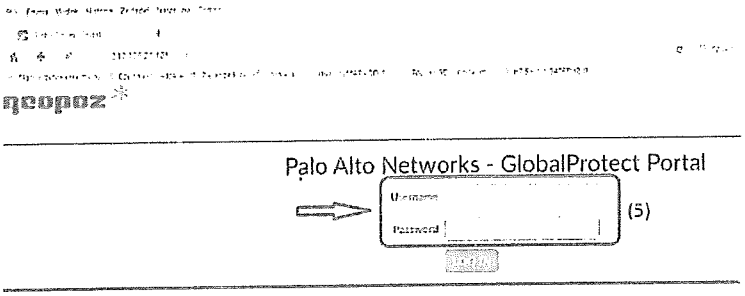




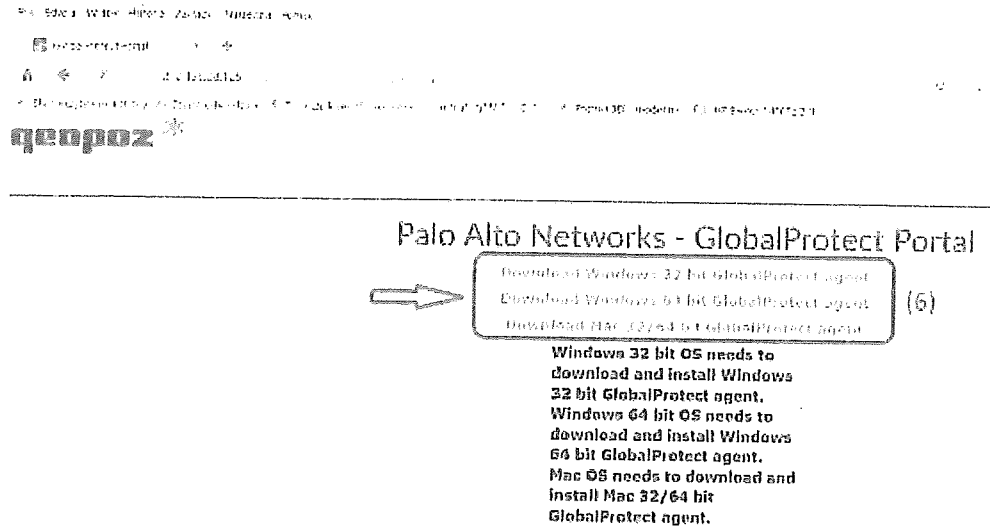
8. W wyświetlonym oknie **Dodanie wyjątku bezpieczeństwa** kliknąć przycisk **Potwierdź wyjątek bezpieczeństwa**.

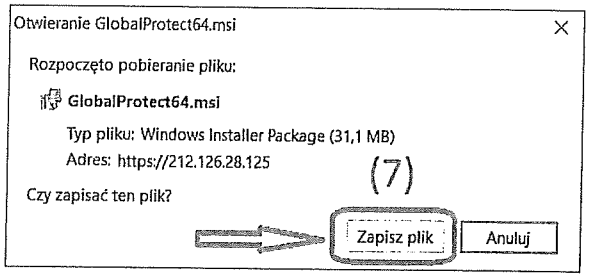


9. Zalogować się wpisując w pola **UserName** i **Password** dane dostarczone przez ZGiKM GEOPOZ (5).

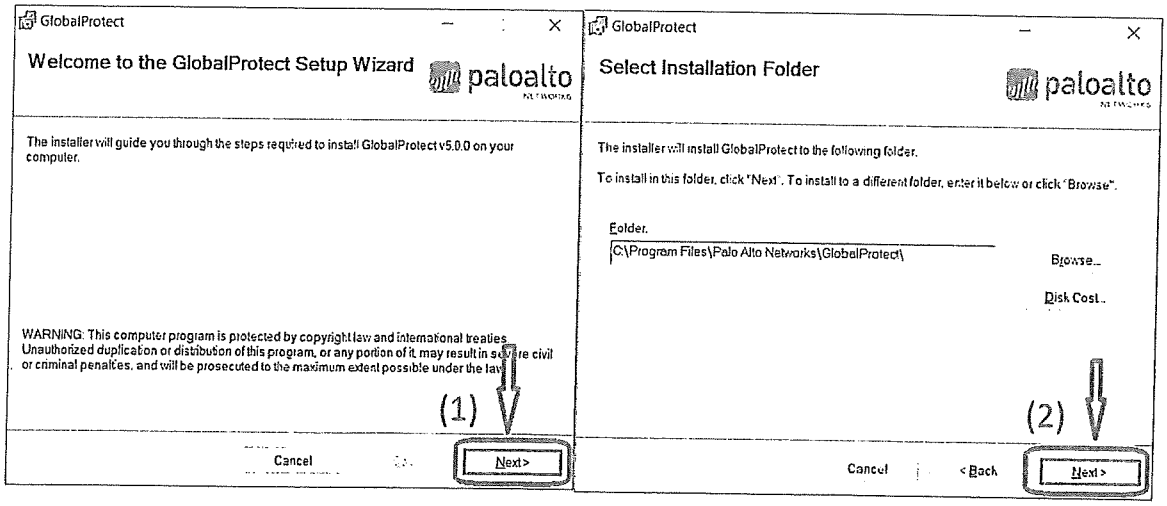


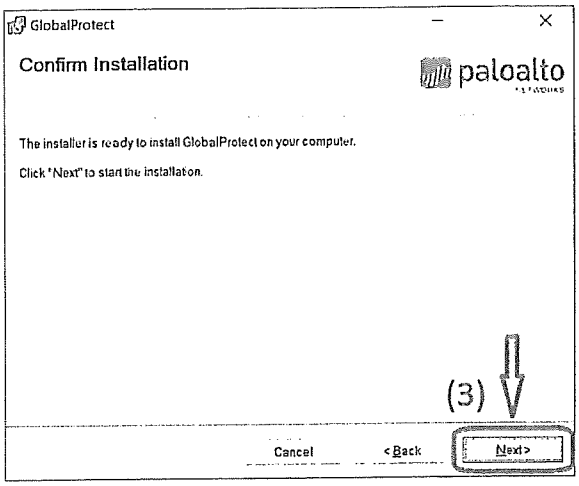
10. Wybrać klienta właściwego dla posiadanego systemu operacyjnego (np. zgodnie z zaleceniami dla Windows 64 bit) i zapisać go na dysku (kroki 6 i 7).





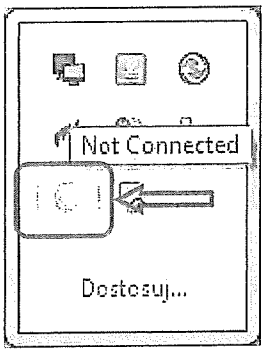
11. Zainstalować wybranego klienta.



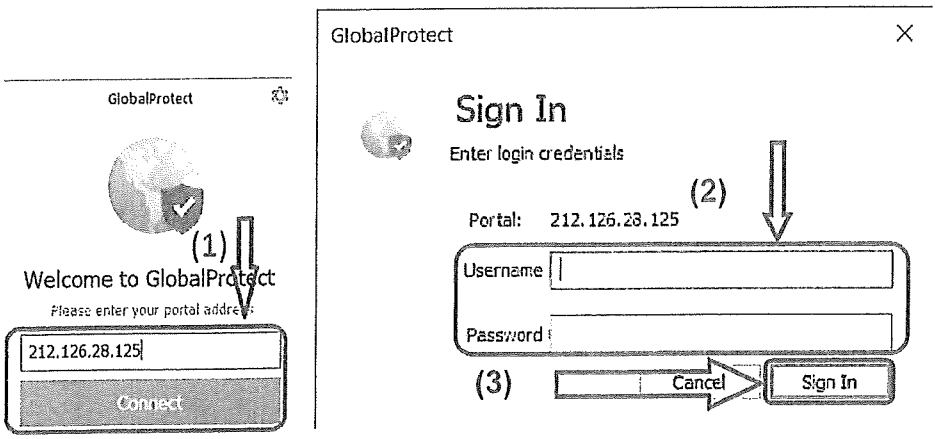


B. Tworzenie tunelu VPN i terminala

1. Aby utworzyć tunel VPN należy uruchomić aplikację **PANGPA.EXE** z lokalizacji C:\Program Files\Palo Alto Networks\GlobalProtect lub kliknąć w obszarze powiadomień ikonkę aplikacji (rys.).

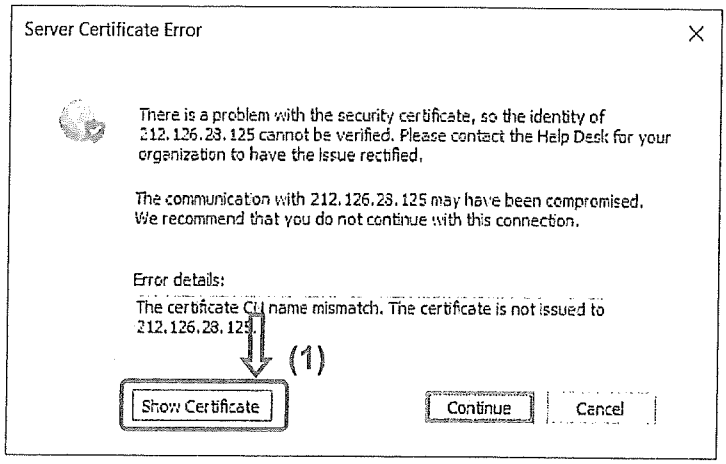


2. Po uruchomieniu wpisać adres portalu **212.126.28.125**, kliknąć **CONNECT** w celu utworzenia tunelu VPN a następnie w oknie logowania wprowadzić nazwę użytkownika oraz hasło i zalogować się (jeśli na stacji był już zainstalowany klient Global Protect to zostaną użyte zapamiętane dane logowania i okno logowania nie pojawi się).

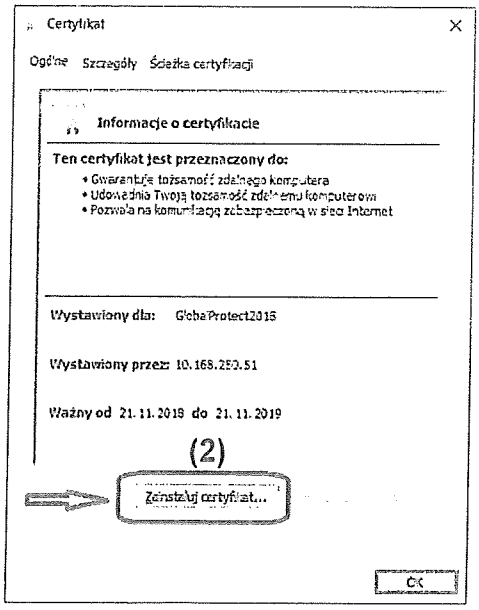


Wprowadzone dane logowania zostaną zapamiętane i będą używane przy kolejnym nawiązywaniu połączenia bez potrzeby ich ponownego wprowadzania.

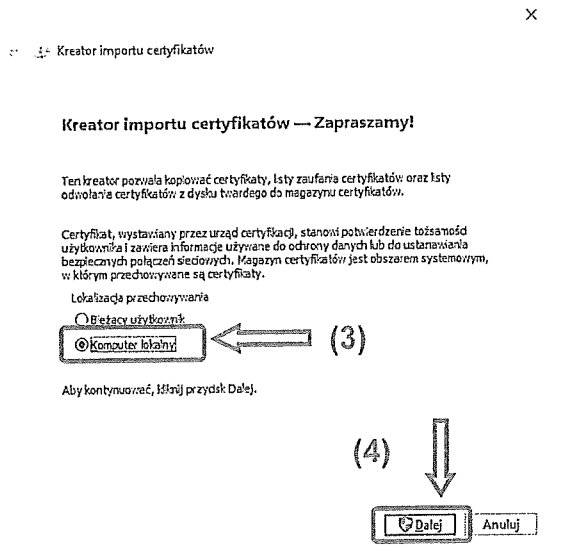
3. Jeżeli pojawi się komunikat o problemie z certyfikatem to kliknąć **Show Certificate**.

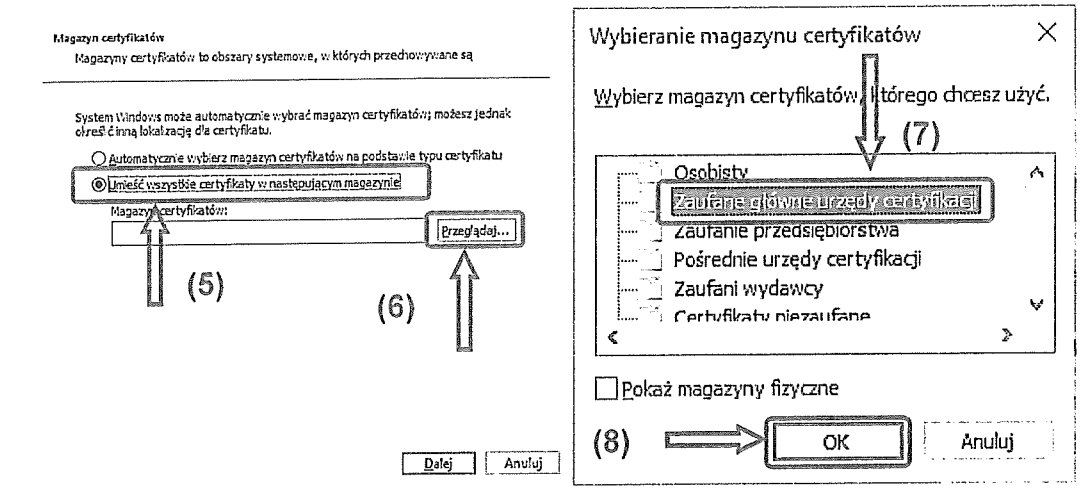


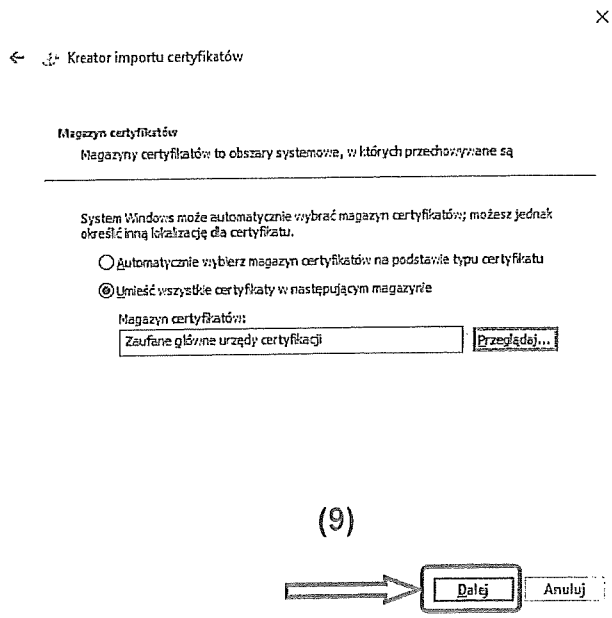
W kolejnym oknie kliknąć **Zainstaluj certyfikat...**

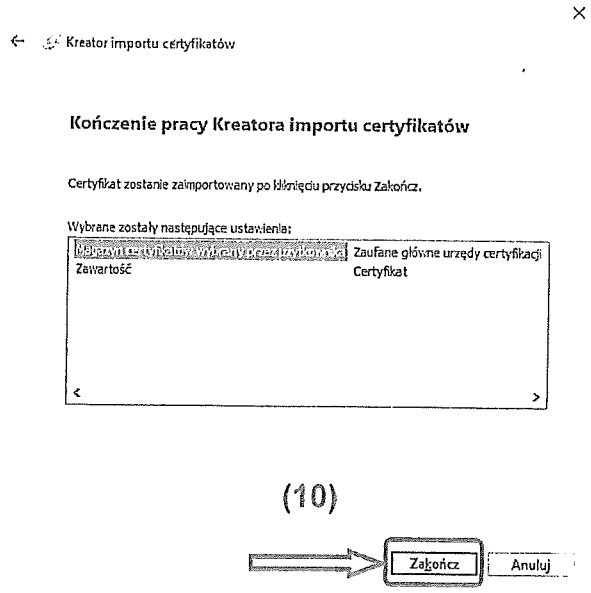


Następnie przejść przez kolejne kroki w **Kreatorze importu certyfikatów**:

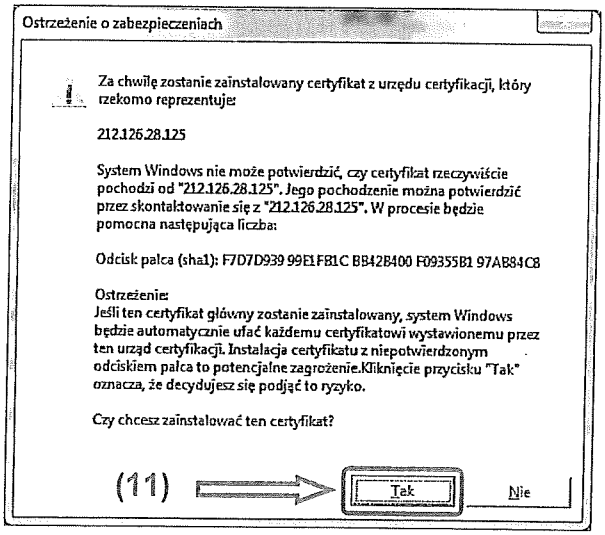

Kreator importu certyfikatów
Kreator importu certyfikatów — Zapraszamy!
Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.
Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, w którym przechowywane są certyfikaty.
Lokalizacja przechowywania
Bieżący użytkownik
Komputer lokalny
(3)
Aby kontynuować, kliknij przycisk Dalej.
(4)
Dalej
Anuluj


Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów:
Przeglądaj...
(5)
(6)
Dalej
Anuluj
Wybieranie magazynu certyfikatów
Wybierz magazyn certyfikatów, którego chcesz użyć.
(7)
Osobisty
Zaufane główne urzędy certyfikacji
Zaufanie przedsiębiorstwa
Pośrednie urzędy certyfikacji
Zaufani wydawcy
Certyfikaty niezaufane
Pokaż magazyny fizyczne
(8)
OK
Anuluj

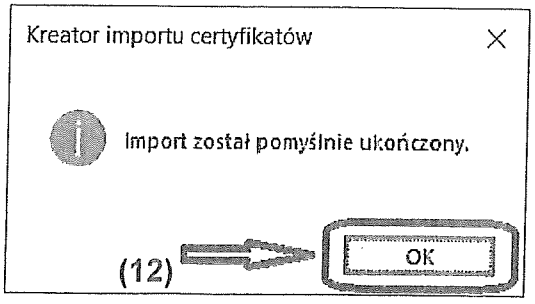

Kreator importu certyfikatów
Magazyn certyfikatów
Magazyny certyfikatów to obszary systemowe, w których przechowywane są
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu
Umieść wszystkie certyfikaty w następującym magazynie
Magazyn certyfikatów:
Zaufane główne urzędy certyfikacji
Przeglądaj...
(9)
Dalej
Anuluj



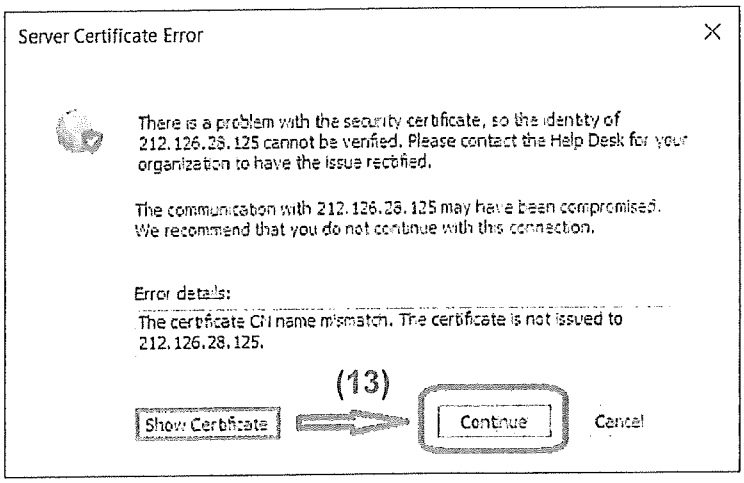
Uwaga: W systemie Windows 10 podczas instalacji certyfikatu pojawia się dodatkowe okno (rys. poniżej), w którym należy potwierdzić instalację przyciskiem **Tak** (11).



Import kończy się komunikatem:

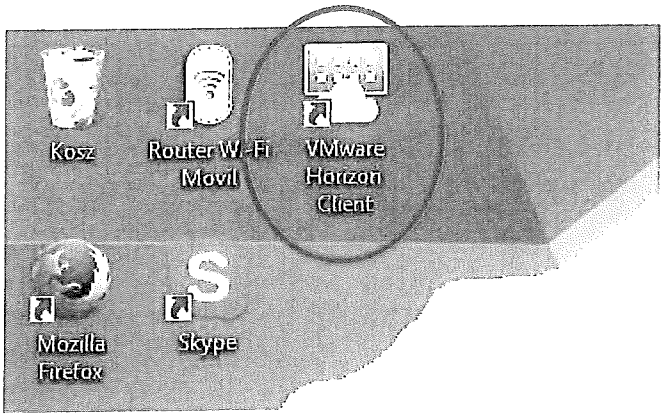


Po jego zatwierdzeniu następuje powrót do okna, z którego został uruchomiony proces instalacji certyfikatu. Okno zamykamy naciskając przycisk **Continue**.

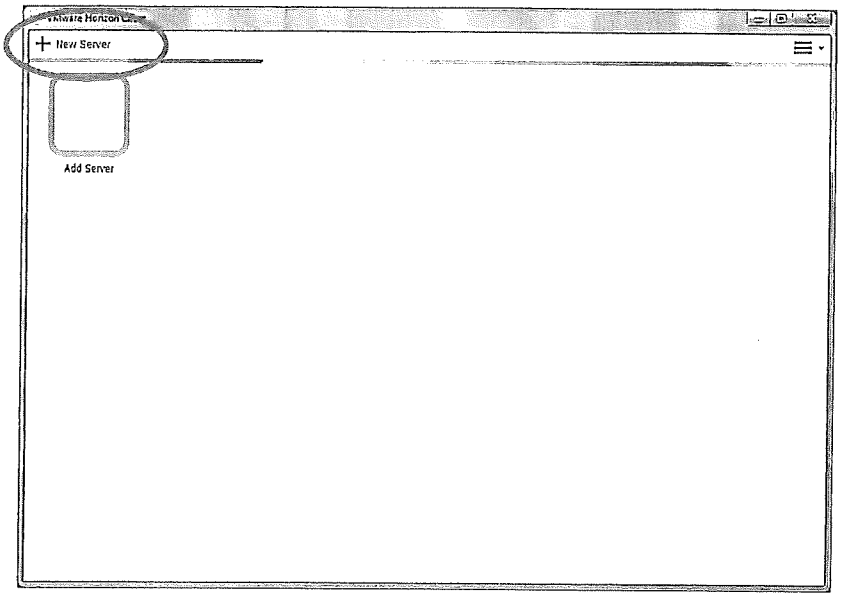


4. Utworzenie tunelu potwierdzone jest statusem **CONNECTED**.

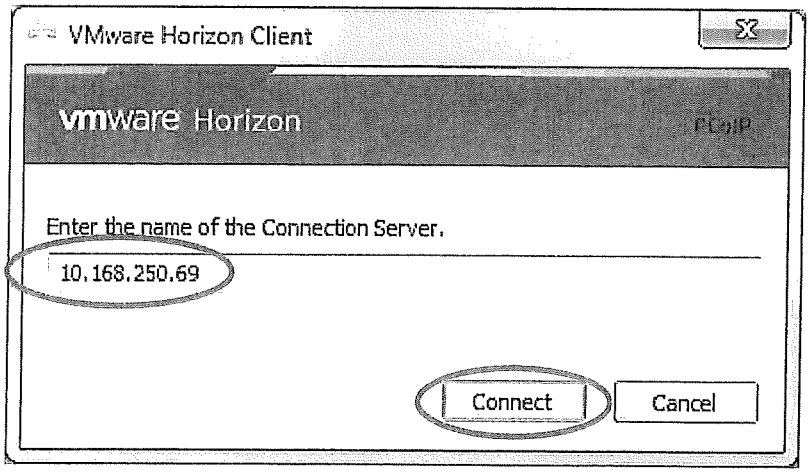
5. Po utworzeniu tunelu VPN należy utworzyć połączenie z serwerem terminali. W tym celu należy uruchomić aplikację **VMware Horizon Client**, do której skrót powinien być na pulpicie.



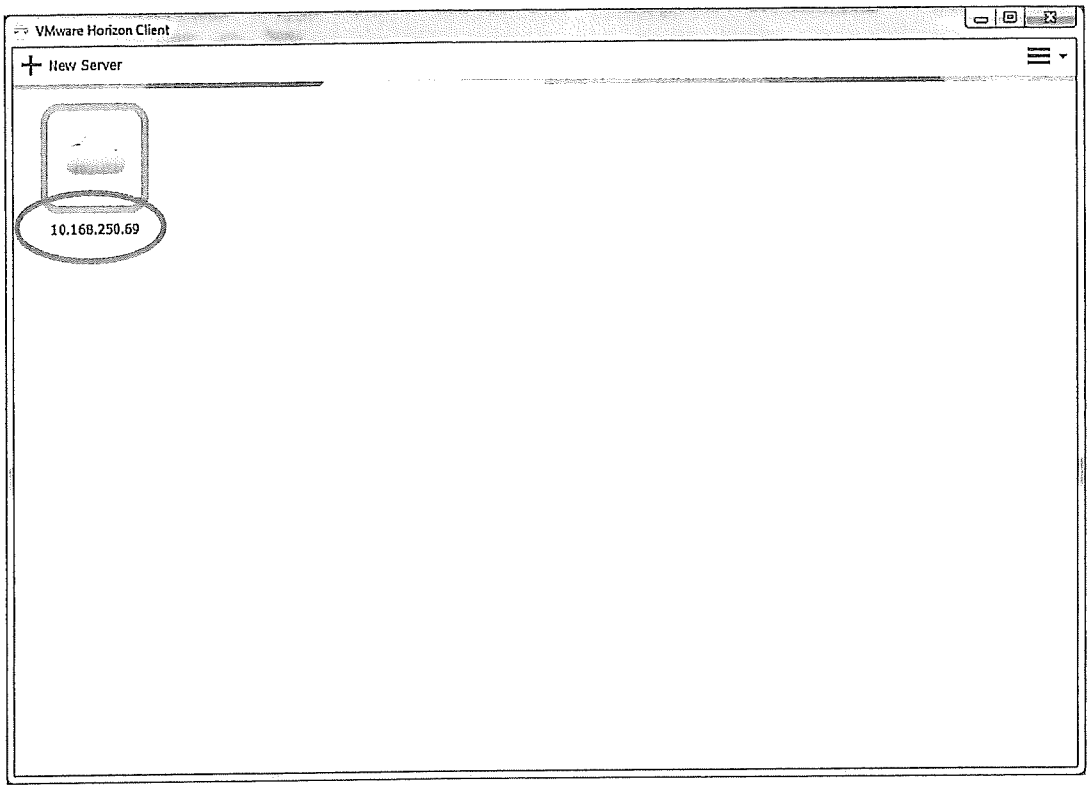
6. W oknie aplikacji wybrać **NEW SERVER**.



7. Wpisać adres serwera **10.168.250.69** i kliknąć **CONNECT**.

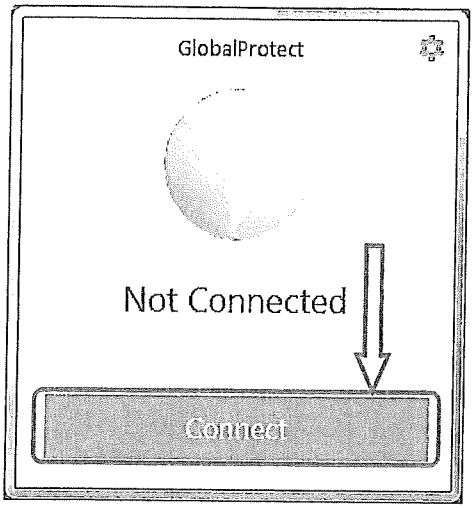


8. Nowy serwer zostanie zapisany.



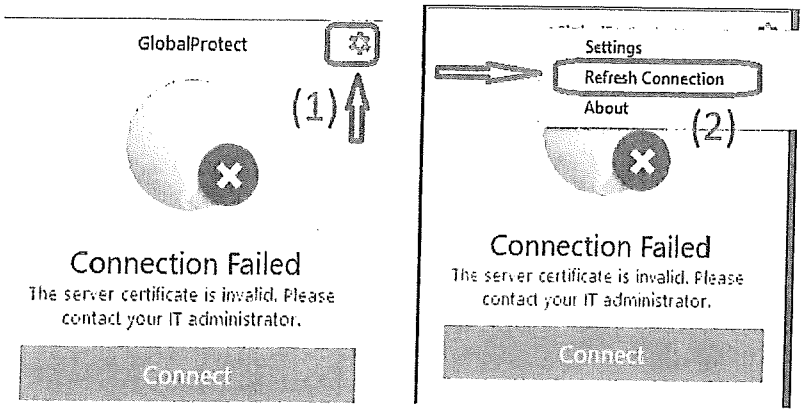
C. Uruchamianie systemu WEGA z terminala

1. Aby ustanowić tunel VPN kliknąć ikonę klienta VPN w obszarze powiadomień, po czym w oknie klienta nacisnąć przycisk **CONNECT**.

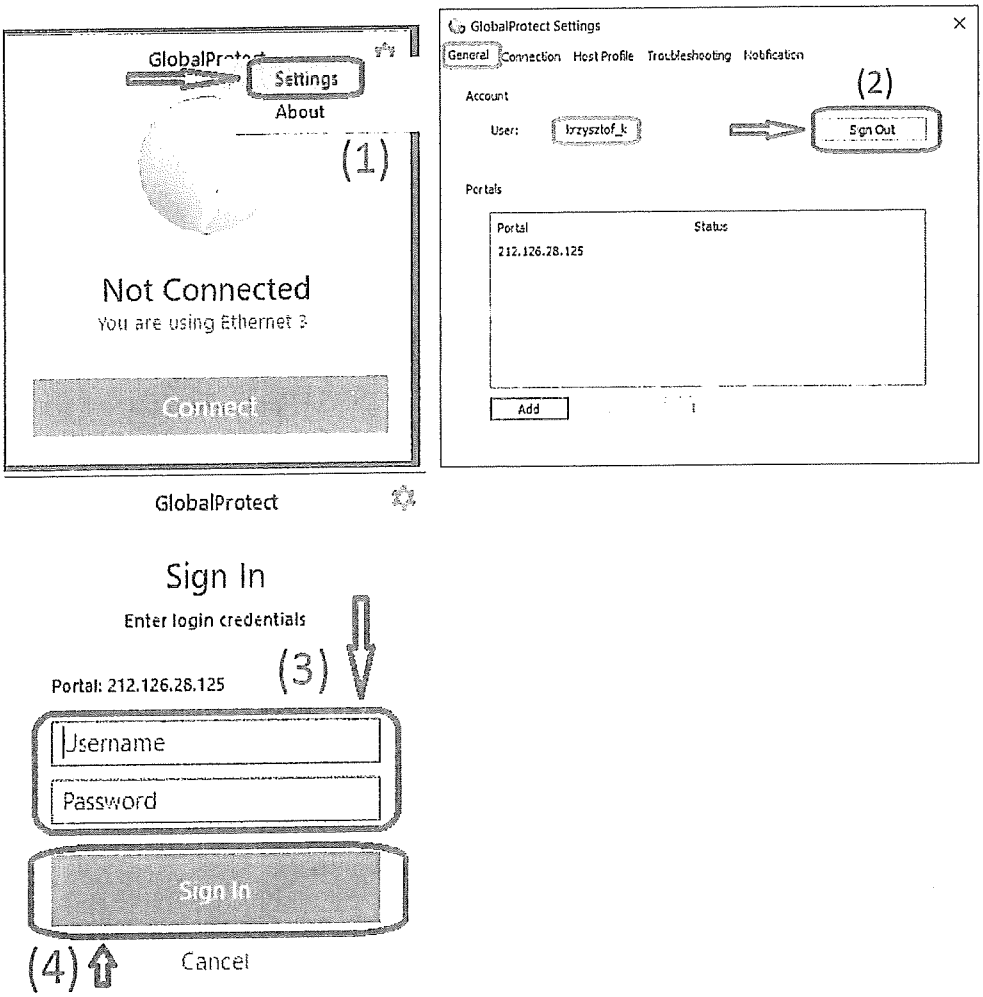


2. Połączenie powinno nastąpić automatycznie.

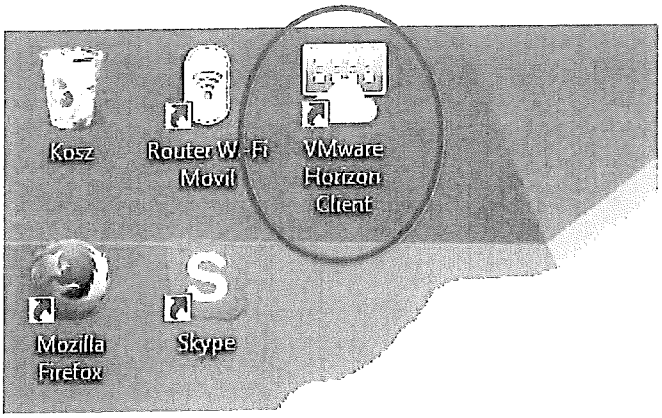
3. W przypadku problemu z certyfikatem serwera (1-szy rysunek poniżej) kliknąć ikonkę ustawień (1), następnie odświeżyć połączenie (2).



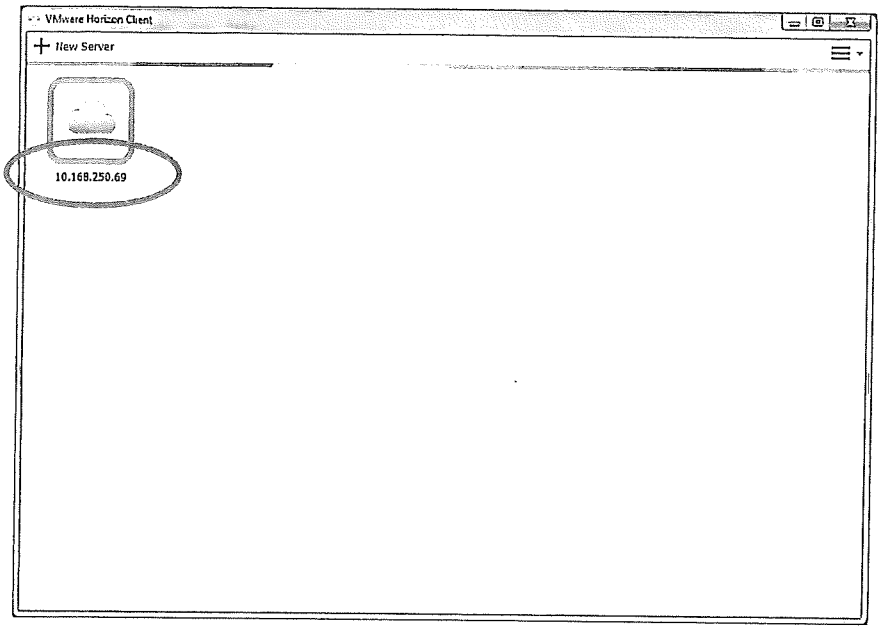
4. W przypadku potrzeby zmiany danych użytkownika wykorzystywanych przy nawiązywaniu połączenia należy wejść w ustawienia (1), usunąć dane bieżącego użytkownika (2), wprowadzić nazwę i hasło nowego użytkownika (3) i zatwierdzić (4).



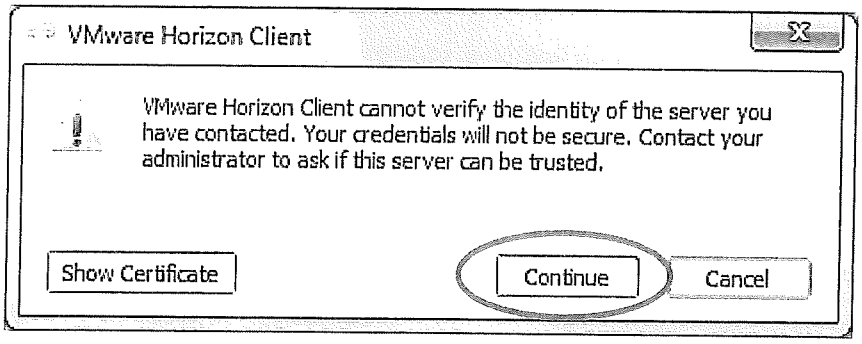
5. Po uzyskaniu połączenia VPN należy uruchomić aplikację **VMware Horizon Client**, do której skrót powinien być na pulpicie.



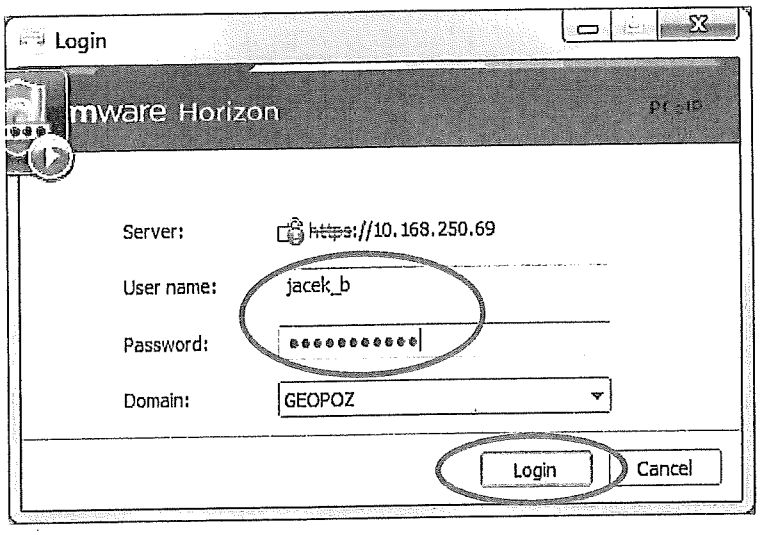
6. Po uruchomieniu wybrać serwer **10.168.250.69**.



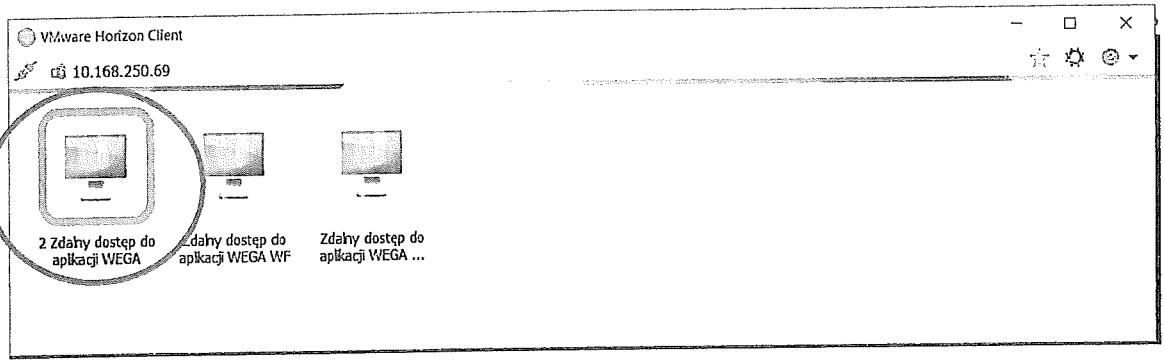
7. Jeżeli pojawi się komunikat o problemie z certyfikatem to kliknąć **CONTINUE**.



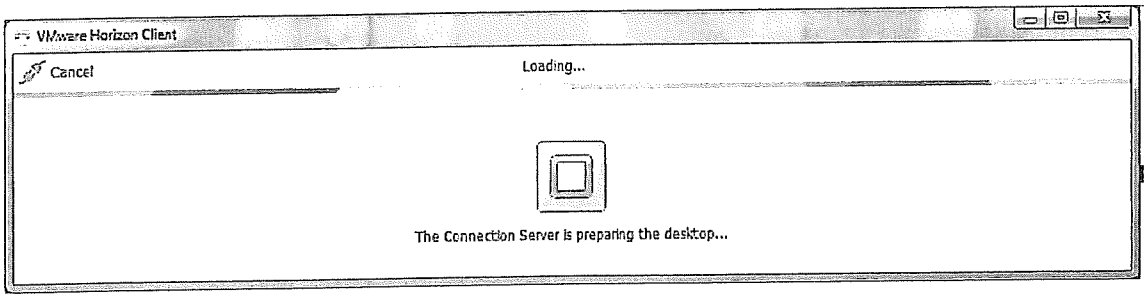
8. W oknie logowania podać użytkownika i hasło takie jak w pkt. A. 9 i kliknąć **LOGIN**.



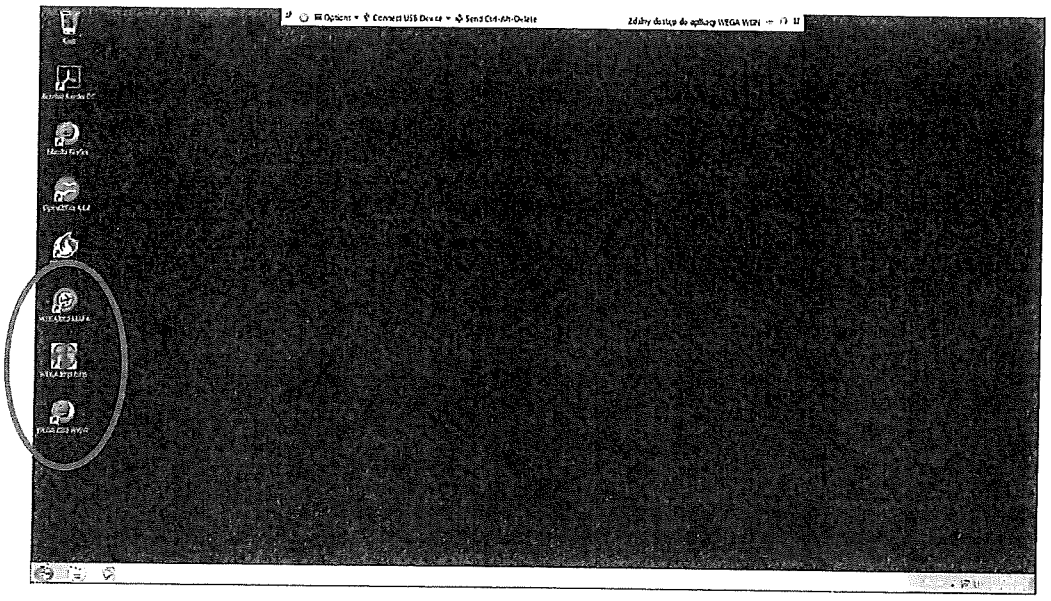
9. W zależności od uprawnień nadanych użytkownikowi ilość dostępnych opcji może być różna. Należy kliknąć na jedną z nich, np. **Zdalny dostęp do aplikacji WEGA.**



10. Przygotowywany jest terminal dla użytkownika.



11. Po poprawnym logowaniu otrzymujemy dostęp do terminala. Klikamy skrót do właściwego modułu systemu WEGA (MAPA, OPIS, WWW) i rozpoczynamy pracę.

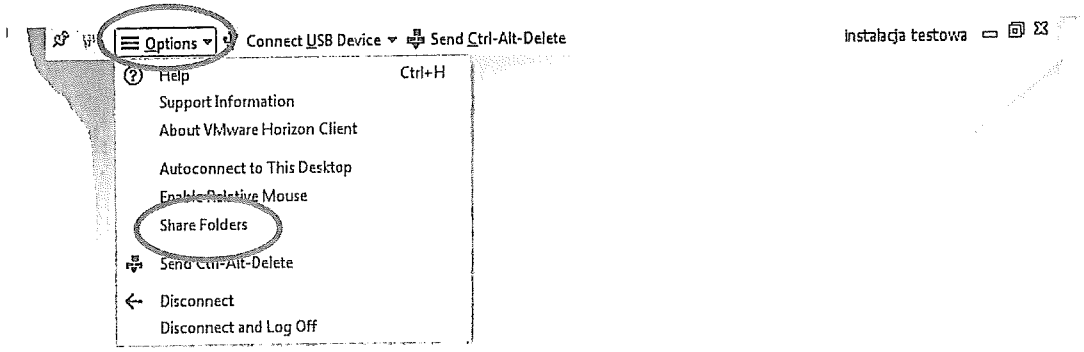


12. Po zakończeniu pracy w systemie WEGA należy wylogować się z terminala (standardowa operacja Windows **START -> WYLOGUJ**).

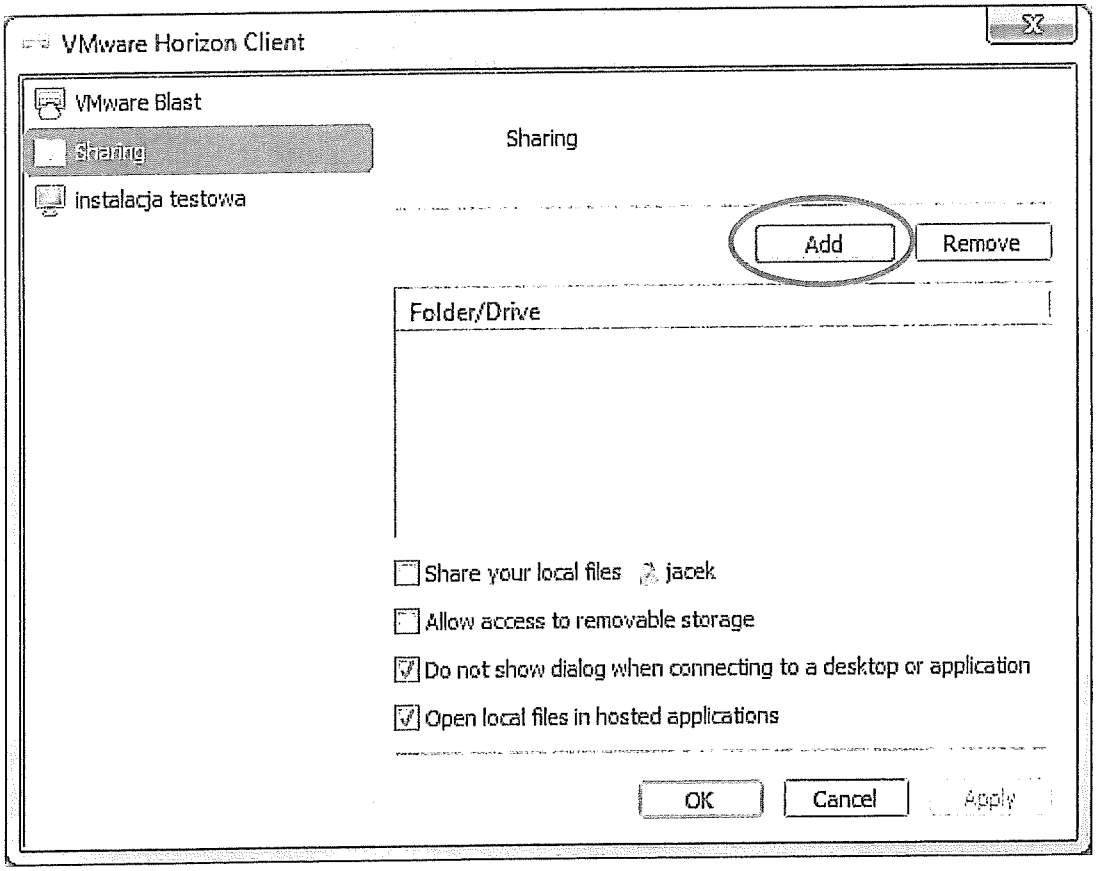
13. Po wylogowaniu z terminala należy zamknąć tunel VPN przez wybranie ikony klienta VPN i naciśnięcie **DISCONNECT**.

D. Udostępnianie dla terminala lokalnych zasobów stacji roboczej

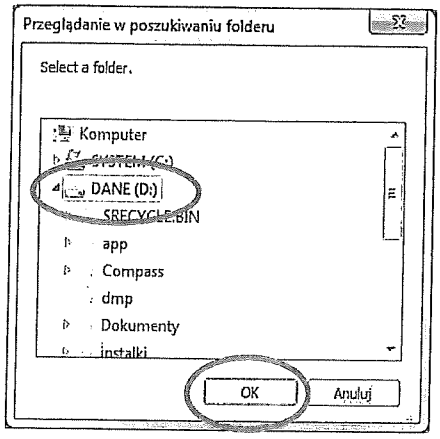
1. Po uruchomieniu terminala można udostępnić lokalne zasoby stacji roboczej tak aby terminal widział np. dyski lokalne komputera, na którym jest zainstalowany klient VPN i terminal. W tym celu należy kliknąć na **Options** i wybrać operację **Share Folders.**



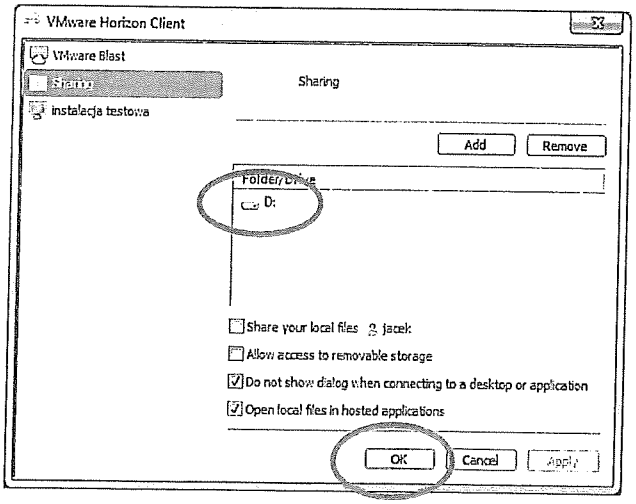
2. Wybieramy katalogi, które chcemy mieć dostępne podczas pracy z terminalem klikając na **Add.**



3. Wskazujemy odpowiedni katalog z naszego komputera (może być wskazany cały dysk, np. dysk D).



4. Wybrany katalog pojawi się na liście udostępnionych zasobów. Aby zakończyć udostępnianie klikamy **OK**. Ustawienia zostaną zapamiętane na przyszłe logowania.



Załącznik nr 9b
do warunków technicznych

WARUNKI TECHNICZNE DOSTEPU DO SYSTEMU WEGA Z WYKORZYSTANIEM DOSTĘPU TERMINALOWEGO ZA POMOCĄ KANAŁU VPN

1. Zamawiający zobowiązuje się do zapewnienia na czas trwania Umowy/Umów zdalnego połączenia do systemu informatycznego Zamawiającego w zakresie i celu realizacji zadań objętych Umową/Umowami.
2. Warunki techniczne korzystania ze zdalnego połączenia do systemu informatycznego Zamawiającego:
   2.1. Ze względów technicznych i organizacyjnych Zamawiającego, praca zdalna może być prowadzona w dniach roboczych w godzinach 8.00-20.00 przy czym w godzinach od 8.00-16.00 Zamawiający zapewnia pomoc telefoniczną swoich pracowników
   2.2. stacja robocza Wykonawcy, z której dokonywane jest połączenie musi posiadać system operacyjny Windows 10 (najlepiej w wersji 64 bitowej)
   2.3. stacja robocza Wykonawcy musi posiadać podłączenie do Internetu
   2.4. Wykonawca oświadcza, że zapewnia środki ochrony technicznej i organizacyjnej danych osobowych stacji roboczej wyznaczonej do realizacji umowy, a w szczególności do wyposażona ww. stacji w oprogramowane zabezpieczające (np. antywirus, ochrona transmisji danych). Za właściwe zabezpieczenie stacji roboczej odpowiedzialny jest Wykonawca.
   2.5. na stacji roboczej Wykonawcy zainstalowane są komponenty wskazane i zainstalowane wg Instrukcji przygotowania środowiska do pracy terminalowej WEGA stanowiącej załącznik do niniejszych Warunków
   2.6. podczas pracy zdalnej, stacja robocza Wykonawcy jest automatycznie odcinana od sieci lokalnej Wykonawcy i możliwe jest korzystanie tylko z zasobów lokalnych stacji roboczej Wykonawcy (dyski, drukarki) oraz zasobów zdalnych udostępnionych przez Zamawiającego.
3. Warunki wydawania uprawnień do pracy zdalnej w systemie informatycznym Zamawiającego dla pracowników Wykonawcy:
   3.1. uprawnienia udzielane są na pisemny wniosek Wykonawcy
   3.2. w przypadku braku możliwości technicznych Zamawiający zastrzega sobie prawo odmowy wydania uprawnień
   3.3. informacje uwierzytelniające (login i hasło) zostaną przekazane Wykonawcy przez Zamawiającego w trybie roboczym

3.4. Wykonawca zapewnia, że do stacji roboczej logują się tylko uprawnione osoby posiadające upoważnienie do przetwarzania danych osobowych wynikające z odrębnie podpisanej umowy powierzenia przetwarzania danych osobowych, stanowiącej załącznik, do Umowy/Umów, o której/których mowa w pkt 1.

4. Zamawiający nie ponosi odpowiedzialności za ewentualne szkody związane z nieprawidłowym funkcjonowaniem systemu informatycznego Wykonawcy spowodowane przerwami w pracy zasobów systemu informatycznego Zamawiającego powstałymi na skutek prac konserwacyjnych, awarii sprzętu sieciowego lub łączy transmisji danych.

5. Wykonawca ponosi odpowiedzialność za spowodowanie naruszenia zasad bezpieczeństwa systemu informatycznego Zamawiającego wynikających z realizacji zadań objętych Umową/Umowami, w tym za:

   5.1. nieautoryzowany dostęp do systemu informatycznego Zamawiającego,

   5.2. szkody powstałe w wyniku nie zastosowania się do warunków technicznych, o których mowa w pkt 2

   5.3. próby badania, skanowania i testowania odporności systemu informatycznego Zamawiającego, mechanizmów autentykacji i luk bez zgody Zamawiającego,

   5.4. celowe obciążanie urządzeń i systemów powodujące degradację usług lub przeciążenie systemu informatycznego Zamawiającego,

6. Zamawiający zastrzega sobie prawo do szczegółowego zbadania przypadków naruszenia bezpieczeństwa systemu informatycznego Zamawiającego, o których mowa w pkt 5.

7. Zamawiający zastrzega sobie prawo jednostronnej zmiany zasad korzystania ze zdalnego połączenia do systemu informatycznego Zamawiającego opisanych w pkt 2. w trakcie trwania Umowy/Umów.

Podpis Wykonawcy

23.03.2020 Anna Gontarska

data, podpis, pieczęć firmowa

PROGETI-ANNA GONTARSKA
95-100 Zgierz ul. Lisia 15
NIP 7321176640 REGON 360154017
TEL. 504 243 772

Załącznik nr 10
do warunków technicznych

Wyciąg z Polityki bezpieczeństwa dot. współpracy z podmiotami zewnętrznymi

V.9 Współpraca z podmiotami zewnętrznymi.

1. W celu utrzymania bezpieczeństwa przetwarzanych w Zarządzie informacji oraz zapewnienia stosowania środków ochrony przez podmioty zewnętrzne, w zakresie udostępnionej przez Zarząd informacji lub środków komunikacji, za pomocą których zarządzają lub przetwarzają w/w informację, określono zasady dostępu podmiotów zewnętrznych do informacji oraz zasobów przeznaczonych do ich przetwarzania, a w szczególności:
   1) zasady dostępu fizycznego do strefy chronionej przetwarzania danych, w tym miejsc przechowywania i przetwarzania danych;
   2) zasady dostępu do Systemu Informatycznego Zarządu, w tym aplikacji i baz danych;
   3) zasady dostępu do zasobów, w tym Systemu Informatycznego Zarządu.
2. Zasady, procedury oraz zakres odpowiedzialności w zakresie współpracy z podmiotami zewnętrznymi zostały określono w rozdziale 0 PBI.
3. Udostępnienie lub powierzenie danych podmiotom zewnętrznym jest realizowane na podstawie umów lub porozumień.
4. Umowy/porozumienia, na podstawie których powierza się lub udostępnia dane osobowe winny zawierać informacje dotyczące:
   1) czasu trwania umowy;
   2) sposobu i miejsca realizacji umowy;
   3) nazwy udostępnionego/ powierzonego zbioru danych osobowych;
   4) zakresu i celu powierzenia/udostępnienia danych osobowych;
   5) zapisów dotyczących wymagań zapewnienia środków technicznych i organizacyjnych dla zapewnienia ochrony danych osobowych - w przypadku powierzenia przetwarzania danych na podstawie 1rt.31 Ustawy;
   6) sposobu przekazania danych w przypadku wydania danych poza obszar chroniony;
   7) danych kontaktowych Administratora Bezpieczeństwa Informacji nadzorującego ochronę danych;
   8) listy osób wyznaczonych/upoważnionych do przetwarzania danych w związku z realizacją umowy;
   9) sposobu postępowania w przypadku naruszenia bezpieczeństwa przetwarzanych danych;
   10) zobowiązania o zachowaniu w poufności przetwarzanych danych w czasie realizacji umowy i po jej zakończeniu oraz zobowiązanie do zwrotu lub zniszczenia danych po zakończeniu realizacji umowy.
5. Realizacja umowy/porozumienia na przetwarzanie zdalne odbywa się na zasadach określonych w rozdziale 0. PBI.
6. W przypadku, gdy umowa/porozumienie będzie realizowane w siedzibie Zarządu na sprzęcie podmiotu zewnętrznego, porozumieniu z Działem Informatyki należy określić na piśmie wymagania dotyczące:
   1) konfiguracji sprzętu – wymogów technicznych sprzętu;
   2) systemu operacyjnego;
   3) wymagań dotyczących oprogramowania do przetwarzania danych.

7. Procedury dotyczące instalacji i dezinstalacji sprzętu dostarczonego przez podmiot zewnętrzny i oprogramowania, określono w rozdziale III.5 Instrukcji Zarządzania SI.

8. Usługi stanowiące zasób niematerialny są świadczone na podstawie zawartych przez Zarząd umów z podmiotami zewnętrznymi i nadzorowane przez:

   1) Dział Administracyjno-Techniczny – w zakresie umów na dostawę mediów tj. prąd, woda, ogrzewanie;
   2) Dział Informatyki – w zakresie umów na obsługę transmisji i prezentacji danych;
   3) ABI – w zakresie bezpieczeństwa przetwarzania danych osobowych oraz zgodności przetwarzania z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami.

V.9.1 Środki ochrony związane z działaniami podmiotów zewnętrznych

1. Osoby odpowiedzialne za współpracę z podmiotami zewnętrznymi są zobowiązane do przedłożenia projektu umowy/porozumienia z:

   1) ABI – w zakresie przetwarzania danych;
   2) Głównym Informatykiem – w zakresie sposobu realizacji pod kątem informatycznym.

   oraz przekazywanie do Głównego Informatyka i ABI kopii zawartych umów/porozumień.

2. W umowach/porozumieniach muszą być zawarte klauzule związane z ochroną danych przetwarzanych w Zarządzie, w tym:

   1) zapewnienia środków technicznych i organizacyjnych przewidzianych w Ustawie w celu zabezpieczenia przetwarzania powierzonych danych osobowych;
   2) zobowiązanie do zachowania w poufności wszystkich informacji, w tym danych osobowych pozyskanych dla potrzeb realizacji umowy i po jej zakończeniu;
   3) zobowiązanie do zniszczenia lub zwrotu powierzonych danych po zakończeniu trwania umowy/porozumienia;
   4) reguły postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa.

3. Wszystkie osoby wskazane do realizacji umowy/porozumienia na przetwarzanie danych osobowych Zarządu muszą posiadać imienne upoważnienia wydane przez AD – zasady wydawania upoważnień określono w Zarządzeniu ODO.

4. Wydanie kluczy do pomieszczeń znajdujących się w strefie przetwarzania danych osobowych określonym w umowie/porozumieniu, odbywa się na podstawie dostarczonej do Działu Administracyjno-Technicznego listy osób wskazanych do jej realizacji, zawierającej:

   1) imię i nazwisko;
   2) nr dowodu osobistego;
   3) nazwę firmy (jeżeli osoba jest pracownikiem firmy trzeciej);
   4) nr pomieszczenia;
   5) terminu realizacji umowy/porozumienia.

5. Dostęp do pomieszczeń wskazanych w umowie/porozumieniu jest realizowany zgodnie z harmonogramem pracy Zarządu. W przypadku pracy poza wskazanym w regulaminie harmonogramem czasu pracy, osoba nadzorująca realizację umowy/porozumienia musi uzyskać zgodę Dyrektora, a po jej otrzymaniu powiadomić Dział Administracyjno-Techniczny i Dział Informatyki – w celu zapewnienia pracy w systemie SI i dostępu do pomieszczeń.

6. Dostęp do SI nadaje AS na podstawie procedury nadawania uprawnień określonej w Instrukcji zarządzania SI.

7. Wszystkie osoby upoważnione do przetwarzania danych muszą zostać zapoznane z zapisami PBI i Instrukcji zarządzania SI, w zakresie obowiązujących w Zarządzie środków ochrony.

9. Korzystanie ze sprzętu dostarczonego przez podmiot zewnętrzny w celu realizacji umowy/porozumienia odbywa się za zgodą AS po uprzednim pisemnym zgłoszeniu przez osobę nadzorującą realizację umowy/porozumienia do Działu Informatyki:

   1) miejsca podłączenia sprzętu;
   2) zakresu aplikacji jakie mają zostać zainstalowane na dostarczonym sprzęcie w związku z realizacją umowy/porozumienia;
   3) podania konta administracyjnego w celu podłączenia sprzętu do SI Zarządu.

10. Warunkiem koniecznym do uzyskania zgody na podłączenie sprzętu do SI Zarządu jest posiadanie aktualnego:

   1) systemu operacyjnego – ustalonego z Działem Informatyki;
   2) systemu antywirusowego lub zgoda na zainstalowanie takiego systemu przez pracowników Działu Informatyki.

11. Instalacji i dezinstalacji sprzętu i oprogramowania dokonują pracownicy Działu Informatyki.

12. Osoba wskazana w umowie/porozumieniu do nadzoru nad jej realizacją jest zobowiązana powiadamiać o zmianach i zakończeniu realizacji umowy/porozumienia w zakresie:

   1) dostępu pomieszczeń – Dział Administracyjno-Techniczny, ABI;
   2) zmiany osób wskazanych do jej realizacji - Dział Informatyki, Dział Administracyjno-Techniczny, Dział Organizacyjny, ABI;
   3) dostępu do SI – Dział Informatyki i ABI;
   4) instalacji i dezinstalacji sprzętu dostarczonego przez wykonawcę – Dział Informatyki i ABI;
   5) zmiany warunków pracy zdalnej – Dział Informatyki i ABI.

V.9.2 Środki ochrony związane z pracą zdalną podmiotów zewnętrznych

1. Umowa/porozumienie na pracę zdalną z podmiotem zewnętrznym, musi zawierać zapisy określające zasady:

   1) dostępu, w tym:
      a) konfiguracji dostępu – kont dostępowych, dostępnych portów i usług,
      b) dni i godzin realizowania dostępu,
      c) kontroli sesji zdalnej;
   2) nadzoru nad realizacją umowy;
   3) odpowiedzialności Zarządu za realizację umowy, w tym zapewnienie:
      a) działania systemów i urządzeń transmisji danych,
      b) dostępu do zasobów niezbędnych do realizacji zawartej umowy/porozumienia;
   4) odpowiedzialności podmiotu zewnętrznego, w tym osób realizujących umowę/porozumienie; w zakresie zachowania:
      a) poufności przetwarzanych danych,
      b) tajemnicy sposobu zabezpieczenia danych i dostępu,
      c) poufności sprzętu na którym będzie realizowany dostęp zdalny – zapewnienie, że dostęp do sprzętu posiadają wyłącznie upoważnione osoby;
   5) powiadamiania i odpowiedzialności za wystąpienie incydentu naruszenia bezpieczeństwa.

2. Zapewnienie dostępu do SI Zarządu oraz zasobów realizuje AS, na wniosek osoby odpowiedzialnej za realizację umowy/porozumienia na zasadach określonych w umowie/porozumieniu, zgodnie z procedurą określoną w Instrukcji zarządzania SI.

V.9.3Odpowiedzialność związana z działaniem podmiotów zewnętrznych

1. Osoba wyznaczona przez Zarząd do nadzoru realizacji umowy/porozumienia, odpowiada za:
   1) pozyskanie od osób wskazanych do realizacji umowy/porozumienia danych, niezbędnych do sporządzenia wniosku, o którym mowa w pkt. 2 oraz podpisanych oświadczeń o zachowaniu w tajemnicy danych zawartych w zbiorach danych osobowych pozyskanych w trakcie realizacji umowy i po jej zakończeniu oraz sposobu zabezpieczenia danych;
   2) wypełnienie dostępnego w aplikacji Mdok „Wniosku o udzielenie/odwołanie upoważnienia do przetwarzania ZDO" i przekazanie go do Działu Organizacyjnego, w celu przygotowania imiennego upoważnienia do przetwarzania danych osobowych wskazanych w treści wniosku zbiorów danych osobowych;
   3) w przypadku przetwarzania danych osobowych powierzonych zgodnie z art. 31 Ustawy, w wyniku zawartej przez Zarząd umowy/porozumienia – uzyskania listy osób upoważnionych przez podmiot zewnętrzny wskazany w umowie/porozumieniu do przetwarzania danych w powierzonym zbiorze danych osobowych;
   4) wystąpienie z wnioskiem do Działu Informatyki o dostęp do aplikacji i zasobów SI Zarządu dla upoważnionych pracowników podmiotów zewnętrznych – jeśli dostęp jest niezbędny dla realizacji umowy/porozumienia;
   5) zapewnienie zapoznania osób upoważnionych wskazanych do realizacji umowy/porozumienia z zasadami i procedurami obowiązującymi w Zarządzie w zakresie ochrony przetwarzania danych osobowych obowiązujących w Zarządzie;
   6) dostarczenie do Działu Administracyjno-Technicznego listy osób realizujących umowę/porozumienie w siedzibie Zarządu, z podaniem:
      a) imienia i nazwiska,
      b) numery dowodu osobistego,
      c) numeru pomieszczenia, w którym będzie realizowana umowa (w celu wydania klucza),
      d) harmonogramu pracy z podaniem dni i godzin;
   7) jeśli realizacja umowy odbywa się na sprzęcie dostarczonym przez podmiot zewnętrzny realizujący umowę/porozumienie – powiadomienie Działu Informatyki (NGI) i ABI zgodnie z zapisami rozdziału V.9 pkt.6 PBI;
   8) przestrzeganie zapisów umowy w zakresie :
      a) sposobu i miejsca przetwarzania,
      b) aktualizacji upoważnień dla osób realizujących umowę,
      c) przestrzegania harmonogramu pracy,
      d) korzystania ze sprzętu komputerowego;
   9) zgłaszanie ABI incydentów naruszenia bezpieczeństwa związanych z realizacją umowy/porozumienia, również tych zgłaszanych przez osoby realizujące umowę/porozumienie, zgodnie procedurą określoną w „Instrukcji postępowania z incydentami".

2. Pracownicy podmiotu zewnętrznego wskazani do realizacji umowy/porozumienia, odpowiadają za:
   1) zachowanie w poufności danych pozyskanych w trakcie trwania umowy/porozumienia i po jej zakończeniu oraz sposobu zabezpieczenia danych;
   2) przestrzegania obowiązujących w Zarządzie zasad i procedur dotyczących ochrony przetwarzania danych;
   3) zgłaszanie osobie wyznaczonej przez Zarząd do nadzoru realizacji umowy/porozumienia, zdarzeń naruszających bezpieczeństwo przetwarzania danych lub łamiące obowiązujące w Zarządzie zasady i procedury;
   4) wykorzystanie sprzętu, aplikacji i danych wyłącznie w zakresie przewidzianym w umowie/porozumieniu;
   5) jeśli realizacja umowy odbywa się zdalnie za pomocą łączy teleinformatycznych, realizujący umowę/porozumienie, odpowiada za:
      a) zachowanie w poufności sprzętu na którym realizowany jest dostęp zdalny - zapewnienie dostępu do sprzętu wyłącznie osobom realizującym umowę,

b) zapewnienie środków ochrony przed nieuprawnionym dostępem, kradzieżą lub modyfikacją danych oraz zabezpieczenie przed działaniem szkodliwego oprogramowania,
c) zachowanie zachowania w poufności zastosowanych środków ochrony i sposobu dostępu.

3. Dział Organizacyjny odpowiada za wydanie, aktualizację i odwołanie upoważnień do przetwarzania danych osobowych na podstawie wniosku osoby nadzorującej umowę/porozumienie.

4. Dział Informatyki odpowiada za instalację i dezinstalację sprzętu i oprogramowania na podstawie pisemnej informacji pozyskanej od osoby nadzorującej realizację umowy/porozumienia, a w przypadku umowy/porozumienia realizowanego zdalnie, odpowiada za:

a) przydzielenie i odebranie dostępu do zasobów i usług określonych w umowie/porozumieniu,
b) nadzorowanie sesji zdalnej przez kontrolę czasu trwania sesji, miejsca nawiązania sesji (IP źródła), użytkownika zestawiającego sesję, zasobu z którym nawiązano połączenie podczas sesji zdalnej – monitorowanie logów systemowych.

5. AS odpowiada za nadanie i odebranie uprawnień dostępu do zasobów SI Zarządu osobom upoważnionym, realizującym umowę/porozumienie. Nadanie uprawnień lub przedłużenie odbywa się zgodnie z procedurą określoną w Instrukcji zarządzania SI.

6. Poszczególni AOU odpowiadają za nadawanie i odbieranie uprawnień dostępu do aplikacji w Systemie SI dla osób upoważnionych wskazanych do realizacji umowy/porozumienia, w zakresie zgodnym z pisemnym wnioskiem osoby nadzorującej jej realizacje.

Załącznik nr 14
do warunków technicznych

pieczęć firmowa

Poznań, ...

ZAWIADOMIENIE

Pan/Pani

.....

.....

..... - .....

W nawiązaniu do zawiadomienia Prezydenta Miasta Poznania z ... 2018 r. informującego o przystąpieniu do modernizacji ewidencji gruntów i budynków w zakresie budynków i lokali położonych na obszarze miasta Poznania w obrębie ewidencyjnym ..... zawiadamia się o konieczności pozyskania przez pracownika firmy ..... z siedzibą ..... danych ewidencyjnych obejmujących informacje dotyczące **budynku** m.in.:

- geometrii, czyli numerycznego konturu budynku,
- pola powierzchni zabudowy,
- procesu budowy, przebudowy, rozbiórki (rok zakończenia budowy, rok zakończenia przebudowy itp.),
- liczby kondygnacji nadziemnych i podziemnych,
- informacji o materiale, z którego zbudowane są zewnętrzne ściany budynku,
- oznaczenia funkcji budynku,
- powierzchni użytkowej.

W związku z powyższym prosi się o udzielenie na terenie Pana/Pani posesji .....*adres budynku*.....dnia.....o godz.....pracownikowi firmy ..... wymaganych informacji .

Pracownicy ww. firmy w trakcie wykonywania prac będą legitymować się zaświadczeniem wydanym przez Geodetę Miejskiego – Dyrektora Zarządu Geodezji i Katastru Miejskiego GEOPOZ oraz imiennym identyfikatorem.

Dane kontaktowe do Wykonawcy – tel. .....

- verte -

Dodatkowe informacje można uzyskać w siedzibie Zarządu Geodezji i Katastru Miejskiego GEOPOZ, na stronie internetowej www.geopoz.pl/bip/ w zakładce ogłoszenia i komunikaty oraz pod numerami telefonów: 618 271 635, 618 271 707, 618 271 600.

Prace związane z modernizacją ewidencji gruntów i budynków wykonywane są na koszt Skarbu Państwa.

Po zakończeniu tych prac, koszt związany z wprowadzeniem nie zgłoszonych lub nieujawnionych danych dotyczących budynku ponosić będzie właściciel/władający.

Zgodnie z art. 22 ust. 2 ustawy z 17 maja 1989 r.- *Prawo geodezyjne i kartograficzne* (Dz.U.2017.2101 z późn. zm.) właściciele nieruchomości mają obowiązek zgłaszania wszelkich zmian danych objętych ewidencją gruntów i budynków w terminie 30 dni od ich powstania, pod groźbą nałożenia grzywny (art. 48 ust. 1 pkt 5 ustawy). Ponieważ zmiany zarejestrowane w ewidencji gruntów i budynków mogą mieć wpływ na wysokość podatku od nieruchomości, w interesie właściciela/użytkownika wieczystego jest poinformowanie również organu ustalającego wymiar podatku o zaistniałej zmianie.

Fundusze Europejskie Program Regionalny

SAMORZĄD WOJEWÓDZTWA WIELKOPOLSKIEGO

Unia Europejska Europejskie Fundusze Strukturalne i Inwestycyjne

Załącznik nr 15 do warunków technicznych

ZG-.... .... .2018

Poznań .....

MONIT

Pan/Pani

ul.
00-000 Poznań

Dotyczy: nieruchomości położonej przy ul. *.....adres budynku...stanowiącej działkę ewidencyjną nr ..., na arkuszu mapy nr ..., w obrębie ewidencyjnym...*

W związku z odmową udzielenia informacji pracownikowi firmy ....., wykonującej modernizację ewidencji gruntów i budynków w zakresie budynków i lokali na obszarze miasta Poznania w obrębie ewidencyjnym ....., Zarząd Geodezji i Katastru Miejskiego GEOPOZ zwraca się z prośbą o skontaktowanie się z przedstawicielem ww. przedsiębiorstwa, w celu uzupełnienia danych ewidencyjnych dotyczących budynku.
Dane kontaktowe do Wykonawcy – tel. ...
Dodatkowe informacje można uzyskać w tut. Zarządzie pod numerami telefonów: **61 82 71 635, 61 82 71 707, 61 82 71 600.**

Na podstawie art. 24a ust. 4 i ust. 6 ustawy z dnia 17 maja 1989 r. – *Prawo geodezyjne i kartograficzne* (Dz.U.2017.2101 ze zm.) po zakończeniu prac, projekt operatu opisowo-kartograficznego będzie podlegał na okres 15 dni roboczych wyłożeniu do wglądu osób fizycznych, osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej, w siedzibie zarządu Geodezji i Katastru Miejskiego GEOPOZ.

Każdy czyjego interesu prawnego dotyczą dane ujawnione w projekcie operatu opisowo-kartograficznego, będzie mógł w okresie wyłożenia do wglądu zgłaszać uwagi do tych danych.

Informacja o terminie i miejscu wyłożenia będzie opublikowana w prasie o zasięgu krajowym i w Głosie Wielkopolskim.

Równocześnie informuję, że prace związane z modernizacją ewidencji gruntów i budynków wykonywane są na koszt Skarbu Państwa. Po zakończeniu tych prac, koszt związany z wprowadzeniem niezgłoszonych lub nieujawnionych danych dotyczących budynku ponosić będzie właściciel/władający.

Ponadto informuję, że zgodnie z art. 22 ww. ustawy właściciele nieruchomości mają obowiązek zgłaszania wszelkich zmian danych objętych ewidencją gruntów i budynków w terminie 30 dni od ich powstania oraz dostarczenia dokumentów niezbędnych do wprowadzenia zmian w ewidencji, pod groźbą nałożenia grzywny (art. 48 ust. 1 pkt 5 ustawy). Ponieważ zmiany zarejestrowane w ewidencji gruntów i budynków mogą mieć wpływ na wysokość podatku od nieruchomości, w interesie właściciela/użytkownika wieczystego jest poinformowanie również organu ustalającego wymiar podatku o zaistniałej zmianie.

Zarząd Geodezji i Katastru Miejskiego GEOPOZ, ul. Gronowa 20, 61-655 Poznań,
tel. +48 61 8271 500, fax +48 61 8230 201, e-mail:geopoz@geopoz.poznan.pl, www.geopoz.pl

Załącznik nr 16
do warunków technicznych

ZG- .....

Województwo: wielkopolskiego
Powiat: Miasto Poznań
Gmina: Miasto Poznań
Jednostka ewidencyjna: Miasto Poznań
Obręb ewidencyjny:
Numer obrębu:

WYKAZ PODMIOTÓW,
KTÓRE ZAPOZNAŁY SIĘ Z DANYMI EWIDENCYJNYMI

Lp.	Data	Imię i nazwisko (właściciela/władającego)	Nr działki/nr arkusza/nr jednostki rejestrowej	Podpis	Uwagi
1	2	3	4	5	6
1.					Z danymi rejestru gruntów /budynków /lokali zapoznałem się Nie wnoszę do nich uwag i zastrzeżeń / Wnoszę uwagi i zastrzeżenia* wyszczególnione w odrębnym wykazie pod pozycją
2.					Z danymi rejestru gruntów /budynków /lokali zapoznałem się Nie wnoszę do nich uwag i zastrzeżeń / Wnoszę uwagi i zastrzeżenia* wyszczególnione w odrębnym wykazie pod pozycją
3.					Z danymi rejestru gruntów /budynków /lokali zapoznałem się Nie wnoszę do nich uwag i zastrzeżeń / Wnoszę uwagi i zastrzeżenia* wyszczególnione w odrębnym wykazie pod pozycją
4.					Z danymi rejestru gruntów /budynków /lokali zapoznałem się Nie wnoszę do nich uwag i zastrzeżeń / Wnoszę uwagi i zastrzeżenia* wyszczególnione w odrębnym wykazie pod pozycją

* - niepotrzebne skreślić

Załącznik nr 17
do warunków technicznych

ZG-.....

Województwo wielkopolskie
Jednostka ewidencyjna: Miasto Poznań
Obręb ewidencyjny:
Numer obrębu:

WYKAZ UWAG I ZASTRZEŻEŃ ZGŁOSZONYCH DO PROJEKTU OPERATU EWIDENCYJNEGO OPISOWO-KARTOGRAFICZNEGO

Lp.	Imię i nazwisko lub nazwa zgłaszającego uwagi i wnioski	Numer jednostki rejestrowej	Szczegółowa treść zgłoszonych uwag i wniosków —————————— data i podpis zgłaszającego	Stanowisko organu prowadzącego ewidencję w sprawie zasadności zgłoszonych uwag i wniosków	Potwierdzenie wprowadzenia zmian do projektu operatu opisowo-kartograficznego
1	2	3	4	5	6

Załącznik nr 3 do Umowy nr ZG-NZP.3420.2.2020 z dn. 23.03.2020 r.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH (Umowa)

zawarta w dniu 23.03.2020 roku, w Poznaniu, pomiędzy:

Miastem Poznań,
reprezentowanym przez:
Dyrektora Zarządu Geodezji i Katastru Miejskiego GEOPOZ z siedzibą przy ul. Gronowa 20, 61-655 Poznań, posiadającym NIP 209-00-01-440; REGON 631257822
w osobie
Andrzeja Krygiera - Geodety Miejskiego, Dyrektora Zarządu Geodezji i Katastru Miejskiego GEOPOZ

zwanym dalej „**Zamawiającym lub Administratorem**"

oraz
Anną Gontarską – Przedsiębiorcą, prowadzącą działalność gospodarczą pod nazwą PROGETI - Anna Gontarska
Z siedzibą w Zgierzu, przy ul. Lisiej 15, 95-100 Zgierz
Nr NIP: 7321176640, Regon: 360154017

zwaną dalej „**Wykonawcą lub Procesorem**"

Administrator i Procesor są zwani dalej łącznie „**Stronami**", a każdy z nich z osobna „**Stroną**".

§ 1
PRZEDMIOT UMOWY

1. Administrator i Procesor zawierają umowę powierzenia przetwarzania danych osobowych, zwaną dalej "Umową", na mocy której Administrator powierza Procesorowi przetwarzanie danych osobowych, w zbiorze danych ewidencji gruntów i budynków, w celu i zakresie niezbędnym do realizacji umowy nr ZG-NZP.3420.2.2020, zawartej pomiędzy Stronami w dniu 23.03.2020 roku, zwanej dalej „Umową główną".
2. Zawarcie niniejszej umowy stanowi jednocześnie modyfikację Umowy głównej w zakresie regulacji zasad przetwarzania danych osobowych.
3. Powierzenie danych osobowych Procesorowi następuje w celu realizacji Umowy głównej *„na wykonanie prac związanych z modernizacją ewidencji gruntów i budynków dla obrębów ewidencyjnych Strzeszyn, Piątkowo"*.
4. Wykaz pracowników, którzy będą uczestniczyć w realizacji umowy, upoważnionych przez Procesora do przetwarzania zbioru danych, stanowi Załącznik do Umowy. Zmiana osób upoważnionych, realizujących umowę nie wymaga aneksu do Umowy.

5. Zakres powierzenia, może zostać w każdym momencie rozszerzony albo ograniczony przez Administratora.
6. Procesor zobowiązuje się przetwarzać powierzone mu dane osobowe wyłącznie w celu i zakresie niezbędnym do realizacji Umowy głównej, przez okres jej trwania Chyba, że dalsze ich przetwarzanie wynika z odrębnych przepisów prawa.

§ 2
OŚWIADCZENIA I OBOWIĄZKI PROCESORA

1. Procesor niniejszym oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie niniejszej Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Procesor oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z:
   1) 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, dalej jako: „RODO");
   2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako: „Ustawa").
2. Procesor jest zobowiązany:
   1) przetwarzać powierzone dane osobowe wyłącznie na podstawie Umowy oraz na udokumentowane polecenie Administratora;
   2) przetwarzać powierzone dane osobowe zgodnie z RODO i z przepisami Ustawy, których Procesor zobowiązany jest przestrzegać, jak również innymi polskimi przepisami przyjętymi w celu umożliwienia stosowania RODO, innymi obowiązującymi przepisami prawa, niniejszą Umową oraz instrukcjami Administratora. Instrukcje (polecenia) są przekazywane przez Administratora drogą elektroniczną (przesyłane na adres e-mail Procesora wskazany w § 9 ust. 3);
   3) udzielać dostępu do powierzonych danych osobowych wyłącznie osobom upoważnionym do ich przetwarzania, w celu wykonywania obowiązków wynikających z Umowy;
   4) zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do bezterminowego zachowania tajemnicy przetwarzanych danych i sposobu ich zabezpieczenia ;
   5) wdrożyć, zgodnie z wytycznymi wskazanymi w § 3 Umowy, odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe będą przetwarzane na podstawie Umowy oraz zapewnić realizację zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych (określonych w art. 25 RODO);
   6) wspierać Administratora (poprzez stosowanie odpowiednich środków technicznych i organizacyjnych) w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO. Współpraca Procesora z Administratorem, w zakresie wskazanym w zdaniu poprzednim, powinna odbywać się w formie i terminie umożliwiającym realizację tych obowiązków przez Administratora; w związku z realizacją tego obowiązku Procesor jest w szczególności zobowiązany do udzielania informacji oraz udostępniania powierzonych danych osobowych (lub ich kopii) na żądanie Administratora w terminie 5

Dni Roboczych w formie określonej przez Administratora w żądaniu; Procesor powinien również niezwłocznie, jednak nie później niż w terminie 2 Dni Roboczych, poinformować Administratora o wniosku dotyczącym realizacji praw osoby, której dane dotyczą, złożonym u Procesora; Procesor nie będzie jednak odpowiadał na taki wniosek bez uprzedniej zgody lub wyraźnego polecenia Administratora;

7) pomagać Administratorowi wywiązać się z obowiązków określonych w RODO (w tym w art. 32–36 RODO), tj. w szczególności w zakresie:
   a) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych;
   b) dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu (obowiązki Procesora w odniesieniu do zgłaszania naruszeń zostały określone w § 7 Umowy);
   c) dokonywania przez Administratora oceny skutków dla ochrony danych oraz przeprowadzania konsultacji Administratora z organem nadzorczym, w tym, w szczególności, jest zobowiązany dostarczać Administratorowi informacji niezbędnych do opisu planowanych operacji przetwarzania oraz celu przetwarzania, a także jest zobowiązany do uczestniczenia w dokonywaniu oceny, czy te operacje są niezbędne oraz proporcjonalne do celu przetwarzania oraz oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą;
8) prowadzić, w formie pisemnej (w tym elektronicznej), rejestr czynności przetwarzania, zawierający informacje o:
   a) nazwie oraz danych kontaktowych Procesora oraz innych podmiotów przetwarzających (w przypadku pod powierzenia danych osobowych, o którym mowa w § 4 Umowy) oraz Administratora, a także inspektora ochrony danych, gdy ma to zastosowanie;
   b) kategoriach przetwarzań dokonywanych w imieniu Administratora;
   c) gdy ma to zastosowanie - przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwie tego państwa trzeciego lub organizacji międzynarodowej;
9) niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub unijnych o ochronie danych; informacja w tym przedmiocie przekazana powinna zostać Administratorowi w formie elektronicznej (na adres kontaktowy e-mail wskazany w Umowie głównej) oraz powinna zawierać stosowne uzasadnienie i wskazanie przepisu prawa, który zdaniem Procesora został naruszony;
10) przechowywać dane osobowe tylko tak długo, jak to określił Administrator lub do czasu realizacji Umowy głównej, chyba, że dalsze przetwarzanie danych będzie uzasadnione odpowiednią przesłanką prawną w tym zakresie.

§ 3
ŚRODKI ORGANIZACYJNE I TECHNICZNE

1. Procesor wdraża i stosuje adekwatne środki techniczne i organizacyjne, w celu zapewnienia stopnia bezpieczeństwa odpowiedniego do ryzyka naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane na podstawie Umowy. Procesor powinien w szczególności wdrożyć – zarówno przy

określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – odpowiednie środki zaprojektowane w celu skutecznej realizacji zasad ochrony danych określonych w RODO oraz w celu ochrony praw osób, których dane dotyczą (zasada ochrony danych osobowych w fazie projektowania określona w art. 25 ust. 1 RODO), a także aby domyślnie przetwarzane były wyłącznie dane osobowe w zakresie zbioru danych ewidencji gruntów i budynków (zasada domyślnej ochrony danych określona w art. 25 ust. 2 RODO).

2. Wdrażając środki organizacyjne i techniczne, o których mowa w ust. 1, Procesor:
   1) przestrzega wytycznych Administratora w zakresie sposobu zabezpieczenia procesów przetwarzania danych osobowych zgodnie z przepisami obowiązującego prawa, o których mowa w § 2 ust. 1 pkt 1 oraz 2;
   2) powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe będzie przetwarzał na podstawie niniejszej Umowy.

§ 4
PODPOWIERZENIE

1. Administrator wyraża zgodę na dalsze powierzenie przez Procesora przetwarzania danych osobowych innym podmiotom przetwarzającym w zakresie oraz celu zgodnym z niniejszą Umową. Procesor jest zobowiązany do informowania o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających. Administrator może sprzeciwić się dalszemu powierzeniu przez Procesora danych osobowych w terminie 7 Dni Roboczych od otrzymania informacji, o której mowa w zdaniu poprzednim. W przypadku wyrażenia sprzeciwu przez Administratora, Procesor nie jest uprawniony do zawarcia umowy z dalszym podmiotem przetwarzającym, którego dotyczy sprzeciw.
2. Procesor zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także chroniło prawa osób, których dane dotyczą.
3. Procesor zapewni, że na podmiot, o którym mowa powyżej, zostaną nałożone obowiązki odpowiadające obowiązkom Procesora określonym w Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
4. Procesor zapewni również w umowie z dalszym podmiotem przetwarzającym możliwość realizacji przez Administratora bezpośredniej kontroli względem dalszego podmiotu przetwarzającego (w tym możliwość przeprowadzania audytów, o których mowa w § 6 Umowy). Procesor jest zobowiązany poinformować dalszy podmiot przetwarzający, że informacje, w tym dane osobowe, na temat tego podmiotu przetwarzającego mogą być udostępnione Administratorowi w celu wykonania przez niego uprawnień, o których mowa w zdaniu poprzedzającym.
5. Procesor jest w pełni odpowiedzialny przed Administratorem za spełnienie obowiązków wynikających z umowy powierzenia zawartej pomiędzy Procesorem, a dalszym podmiotem przetwarzającym. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego dalszego podmiotu przetwarzającego spoczywa na Procesorze.

§ 5
TRANSFER DANYCH OSOBOWYCH

Procesor nie może przekazywać (transferować) powierzonych danych osobowych do państwa trzeciego, znajdującego się poza Europejskim Obszarem Gospodarczym („EOG")

§ 6
AUDYT

1. Administrator poinformuje Procesora co najmniej na 7 Dni Roboczych przed planowaną datą audytu o zamiarze jego przeprowadzenia. Jeżeli z ważnych powodów, w ocenie Procesora, audyt nie może zostać przeprowadzony we wskazanym terminie Procesor powinien poinformować o tym fakcie Administratora, wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.
2. Audyt, o których mowa w § 6 ust. 1, może być wykonany przez Administratora w miejscu przetwarzania danych osobowych objętych powierzeniem w Dni Robocze w godzinach od 9 do 16.
3. Procesor ma obowiązek współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących dane osobowe oraz informacje o sposobie przetwarzania danych osobowych, infrastruktury teleinformatycznej oraz systemów IT, a także do osób mających wiedzę na temat procesów przetwarzania danych osobowych realizowanych przez Procesora.
4. Koszty związane z przeprowadzeniem audytu ponosi podmiot, który zlecił przeprowadzenie audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.

§ 7
ZGŁASZANIE NARUSZEŃ

1. Po stwierdzeniu naruszenia ochrony powierzonych mu przez Administratora danych osobowych Procesor, bez zbędnej zwłoki - jednak nie później niż w terminie 36 h od momentu stwierdzenia naruszenia, zgłasza je Administratorowi. Zgłoszenie powinno zawierać co najmniej informacje o:
   1) dacie, czasie trwania oraz lokalizacji naruszenia ochrony danych osobowych;
   2) charakterze i skali naruszenia, tj. w szczególności o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów danych osobowych, których dotyczy naruszenie, a w razie możliwości, także wskazania podmiotów danych, których dotyczyło naruszenie;
   3) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku z przetwarzaniem danych w systemie informatycznym);
   4) przewidywanym czasie potrzebnym do naprawienia szkody spowodowanej naruszeniem;
   5) charakterze i zakresie danych osobowych objętych naruszeniem;
   6) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
   7) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych;

8) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.

2. Do czasu uzyskania instrukcji od Administratora, Procesor bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
3. Procesor jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Procesor jest zobowiązany na każde żądanie Administratora niezwłocznie udostępnić mu dokumentację, o której mowa w zdaniu poprzedzającym.

§ 8
CZAS TRWANIA UMOWY ORAZ ZASADY ODPOWIEDZIALNOŚCI

1. Niniejsza Umowa przestaje obowiązywać wraz z zakończeniem obowiązywania Umowy głównej.
2. Administrator może rozwiązać Umowę z zachowaniem okresu wypowiedzenia odpowiadającemu okresowi przewidzianemu dla wypowiedzenia Umowy głównej.
3. Po zakończeniu obowiązywania Umowy Procesor powinien zgodnie z dyspozycją Administratora zwrócić lub zniszczyć, w sposób i w terminie odrębnie ustalonym z Administratorem, wszelkie dane osobowe i ich kopie, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. Koszty zwrotu lub zniszczenia danych osobowych oraz ich kopii ponosi Procesor.
4. W przypadku ograniczenia zakresu powierzenia przetwarzania przez Administratora, w trybie określonym w Umowie, postanowienia o rozwiązaniu Umowy stosuje się odpowiednio do danych, które wskutek ograniczenia zakresu nie mogą już być przetwarzane przez Procesora.

§ 9
ADRESY STRON I DANE OSÓB

1. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na adresy Stron wskazane w Umowie głównej.
2. Procesora w kontaktach z Administratorem oraz Administratora w kontaktach z Procesorem w zakresie ustaleń Umowy reprezentować będą osoby wskazane w Umowie głównej.
3. Dane powołanego Inspektora Ochrony Danych Stron:
   a. Administrator – pani Renata Promis, tel. 61 8271-873, adres e-mail: iod@geopoz.poznan.pl
   b. Procesor – ANNA GONTARCZYK, TEL. 504243772, biuro@mogeti.pl

§ 10
POSTANOWIENIA KOŃCOWE

1. Niniejsza Umowa podlega prawu polskiemu. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej Strony.
2. W sprawach, które nie zostały uregulowane Umową, znajdują zastosowanie odpowiednie przepisy Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów z zakresu ochrony danych osobowych.

3. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności, z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
4. Procesor nie może przenieść praw lub obowiązków wynikających z niniejszej Umowy bez pisemnej zgody Administratora.
5. O ile Umowa główna nie stanowi inaczej, wszelkie spory w związku z niniejszą Umową zostaną poddane pod rozstrzygnięcie sądu powszechnego miejscowo właściwego ze względu na siedzibę Administratora.
6. Właściwym do rozstrzygania sporów wynikających z Umowy jest prawo polskie.

DYREKTOR

Administrator

Procesor

PROGETI-ANNA GONTARSKA
95-100 Zgierz
NIP 7321176640 REGON 360154017
TEL. 504 243 772

Specjalista
Ewa Studzińska

Załącznik do Umowy powierzenia przetwarzania danych osobowych

Wykaz pracowników:

Lp.	Nazwisko	Imię	Nr dowodu osobistego
1.	GONTARSKA	ANNA	AYX 388822
2	BUKO	EWELINA	AYI 073130
3	BŁASZKIEWICZ	MONIKA	CFD 172994

Oświadczam, że zgodnie z art.

Zgodnie z art. 29 ust. 3a uPzp wykonawca lub podwykonawca jest obowiązany do zatrudniania na podstawie umowy o pracę, w pełnym wymiarze czasu pracy (pełen etat), z uwzględnieniem minimalnego wynagrodzenia za pracę ustalonego na podstawie art. 2 ust. 3-5 ustawy z dnia 10 października 2002 r. *o minimalnym wynagrodzeniu za pracę* osób wykonujących geodezyjne pomiary terenowe. Wykonawca będzie zobowiązany do przedstawienia Zamawiającemu najpóźniej w dniu podpisania umowy wykazu osób - deklaracji w zakresie sposobu zatrudnienia osób, uprawnień, wiedzy i doświadczenia (załącznik nr 9 do Umowy) wraz z dokumentami potwierdzającymi zatrudnienie tych osób. Wykonawca będzie zobowiązany do przedłożenia Zamawiającemu raz na 3 miesiące przez cały okres realizacji zamówienia wykazu osób - deklaracji w zakresie sposobu zatrudnienia osób realizujących przedmiot zamówienia i otrzymywania przez nie wynagrodzenia wraz z dokumentami potwierdzającymi zatrudnienie tych osób. Zamawiający ustanawia nakaz osobistego wykonania świadczenia przez osoby wskazane w załączonym do Umowy wykazie osób - deklaracji.

Anna Gontarska

PROGETI-ANNA GONTARSKA
95-100 Zgierz ul. Lisia 15
NIP 7321176640 REGON 360154017
TEL. 504 243 772