DO.230.16.2022.ID Oświęcim, 08.04.2022r.

Warunki przetargu
Postępowanie o udzielenie zamówienia publicznego, którego wartość nie przekracza kwoty 130 000 złotych i do którego zgodnie z art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019r. – Prawo zamówień publicznych (t.j. Dz.U. z 2021r. poz. 1129 z późn. zm.) nie stosuje się w/w ustawy

I. Nazwa i adres Zamawiającego
1. Zamawiający: Powiatowy Urząd Pracy w Oświęcimiu.
2. Adres: ul. Wyspiańskiego 10, 32-600 Oświęcim.
II. Tryb udzielenia zamówienia
Postępowanie zostanie przeprowadzone w trybie **przetargu zgodnie z** art. 70^1 - 70^5 Kodeksu Cywilnego.
III. Opis przedmiotu zamówienia:
Aktualizacja 100 licencji oprogramowania Bitdefender GravityZone Elite do wersji Bitdefender GravityZone Ultra XEDR (z modułem EDR) i zakup na kolejny trzyletni okres liczony od 27.09.2022r. - 100 licencji oprogramowania Bitdefender GravityZone Ultra XEDR (z modułem EDR) oraz zapewnienie w w/w okresie wsparcia technicznego.
W ramach okresu wsparcia Zamawiający wymaga (bez dodatkowych opłat): Dostarczania w sposób automatyczny nowych wersji zbiorów (bibliotek), zawierających definicje wirusów komputerowych, umożliwiających wykrywanie i usuwanie wszystkich znanych producentowi programu wirusów komputerowych oraz wszystkich poprawek lub uaktualnień programu w szczególności usuwających wykryte podczas eksploatacji programu błędy lub poprawiających skuteczność wykrywania i usuwania złośliwego oprogramowania.

Dopuszcza się składanie ofert równoważnych. Za równoważną zamawiający uważa ofertę (produkt) posiadający parametry i funkcjonalności takie same lub wyższe (lepsze) niż wskazane poniżej w szczególności produkt równoważny musi posiadać następujące parametry techniczne, funkcjonalności, technologie i rozwiązania:

Użyte rozwiązania i technologie:
- antimalware,
- antispyware,
- dwukierunkowy firewall,
- IDS,
- szczepionka antyransomware,
- skanowanie usb,
- filtr stron,
- kontrola urządzeń,
- kontrola aplikacji i kontrola użytkownika,
- ochrona urządzeń mobilnych,
- ochrona exchange,
- hyperdetect,
- sandbox pro w konsoli,
- inteligentne scentrolizowane skanowanie,
- SVE,
- konsola zarządzająca do wyboru: lokalna lub webowa

Maszyny Wirtualne:
1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu)
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
4. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
5. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
6. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
7. Możliwość wskazania do jakiego serwera ochrony mają się łączyć klienci maszyn wirtualnych.
8. Zapewnia integruję z nieograniczoną liczbą instancji VMWare vCenter, uwzględniając polityki bezpieczeństwa bazujące na obiektach takich jak pule zasobów, foldery i sieci dystrybucyjne.

Serwery Windows :
1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hackerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie powinno zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie powinno posiadać możliwość zablokowania hasłem odinstalowania programu.
9. Sygnatury baz antywirusowych powinny być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie powinno posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików.

Ochrona Exchange :
1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.
5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.

8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy

Konsola zdalnej administracji:

1. Dwa typy konsoli administracyjnej:
• Konsola 1 – serwer administracyjny po stronie producenta
• Konsola 2 – lokalny serwer administracyjny
2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.
3. Możliwość integracji z kontem Domenowym Active Directory w obu rodzajach konsoli.
4. W Konsoli 1 musi być dostępna co najmniej jedna maszyna integrująca z domeną Active Directory.
5. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
16. Serwer centralnej administracji musi posiadać funkcje przełączenia się między widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
17. Po instalacji oprogramowania antywirusowego nie będzie wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm.
19. W całym okresie trwania subskrypcji użytkownik musi mieć prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
20. Możliwość synchronizacji serwera administracyjnego z Active Directory
21. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
22. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
23. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
24. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
25. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
26. Wykorzystanie nie relacyjnej bazy danych MongoDB w serwerze zarządzania.
27. Możliwość przypisywania polityk w zależności na jakim połączeniu użytkownik się znajduje (wifi, sieć przewodowa), DNS, IP, Brama itp.
28. Integracja z zewnętrznym serwerem Syslog w wersji on premis
29. Integracja z Amazon Web Services w wersji chmurowej
30. Integracja z ConnectWise w wersji chmurowej

31. Intergracja z Azure
32. Inetgracja z Nutanix
33. Integracja z Amazon
34. Uwierzytelnianie dwuskładnikowe
35. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
36. Użytkownik na punkcie końcowym musi mieć możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)
37. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
38. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
39. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.

Wsparcie dla :

Windows Desktop
Windows 10 October 2018 Update (version 1809), Windows 10 April 2018 Update (version 1803), Windows 10 Fall Creators Update (version 1709), Windows 10 Creators Update (version 1703), Windows 10 Anniversary Update (version 1607), Windows 10 November Update (version 1511), Windows 10 (RTM, version 1507), Windows 8.1, Windows 8, Windows 7
Windows Tablet and Embedded
Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7
Windows Server
Windows Server 2019, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2
macOS
macOS Catalina (10.15), macOS Mojave (10.14), macOS High Sierra (10.13.x), macOS Sierra (10.12.x), OS X El Capitan (10.11.x), OS X Yosemite (10.10.5), OS X Mavericks (10.9.5)
Linux
Ubuntu 14.04 LTS lub nowszy, Red Hat Enterprise Linux / CentOS 6.0 lub nowszy, SUSE Linux Enterprise Server 11 SP3 lub nowszy, OpenSUSE Leap 42.x, Fedora 25 lub nowszy, Debian 8.0 lub nowszy, Oracle Linux 6.3 lub nowszy, Amazon Linux AMI 2016.09 lub nowszy

Oprogramowanie (lub dodatkowy moduł oprogramowania) musi:

Umożliwiać stałą analizę ryzyka organizacyjnego, aby identyfikować zagrożenia, ustalać priorytety i dostarczać wskazówek dotyczących ograniczania ryzyka związanego z użytkownikami, siecią i punktami końcowymi.
Wykrywać w czasie rzeczywistym zaawansowane zagrożenia, w tym ataki bezplikowe, oprogramowanie ransomware i inne zagrożenia 0-day.
Przetwarzać zdarzenia w punktach końcowych w formie incydentów z określeniem ich priorytetu w celu dodatkowego zbadania i reakcji.
Prowadzić stałe monitorowanie zdarzeń w punktach końcowych, w ramach którego przekazywane są one do analizy w celu stworzenia wizualizacji etapów przebiegu ataku.
Umożliwiać automatyczne detonowanie podejrzanych plików w zamkniętym środowisku wirtualnym.
Umożliwiać przeszukiwanie bazy danych zdarzeń, aby wykryć zagrożenia.
Umożliwiać wizualizację - tj. dawać możliwość graficznego przedstawienia zdarzenia odnotowanego przez system co pozwoli na większą kontrolę nad bezpieczeństwem w środowisku oraz pozwoli na podejmowanie szybkich działań.
Umożliwiać zatrzymanie się rozprzestrzeniania podejrzanych plików lub procesów na inne komputery.
Umożliwiać natychmiastowe zakończenie podejrzanych procesów.
Umożliwiać blokowanie połączenia do i z punktu końcowego w celu zatrzymania ruchu bocznego i dalszych naruszeń podczas badania incydentów.

Umożliwiać wykonywanie poleceń zdalnie na dowolnej stacji roboczej w celu natychmiastowej reakcji na bieżące incydenty.
Posiadać konfigurowalne pulpity nawigacyjne oraz wszechstronne możliwości natychmiastowego i zaplanowanego raportowania.

Ponadto w przypadku jeżeli zastosowanie zaoferowanego rozwiązania równoważnego będzie wymagało odinstalowania dotychczas użytkowanego antywirusa oraz zainstalowania antywirusa innego rodzaju Zamawiający wymaga:

1. Odinstalowania użytkowanego oprogramowania ze wszystkich stacji roboczych w dwóch lokalizacjach (Siedziba PUP w Oświęcimiu i Filia PUP w Kętach).
2. Zainstalowania i konfiguracji oprogramowania na wszystkich stacjach roboczych w dwóch lokalizacjach (Siedziba PUP w Oświęcimiu i Filia PUP w Kętach).
3. Przeszkolenia - min. 6 godzin zegarowych dwóch osób z zakresu obsługi i konfiguracji antywirusa.

Uwaga: Zamawiający ze względów bezpieczeństwa nie dopuszcza zdalnego wykonania operacji o których mowa powyżej w pkt 1 i 2. Odinstalowanie, zainstalowanie oraz konfiguracja musi być przeprowadzona osobiście przez pracowników Wykonawcy w siedzibie PUP w Oświęcimiu i Filii PUP w Kętach pod nadzorem wyznaczonych pracowników Zamawiającego. Dokonanie czynności o których mowa powyżej w pkt 1 i 2 poprzedzi zawarcie z Zamawiającym odpowiedniej umowy z zakresu ochrony danych osobowych (RODO).
Uwaga: Jeżeli Wykonawca wykona czynności o których mowa w pkt 1 i pkt 2 przed 27.09.2022r. to trzyletni okres realizacji zamówienia liczony jest od dnia 27.09.2022r.
Uwaga: Wykazanie równoważności to obowiązek wykonawcy. **Ciężar dowodu wykazania równoważności spoczywa na wykonawcy wykonawca może tego dokonać np. poprzez porównanie funkcjonalności, parametrów technicznych oferowanego oprogramowania w stosunku do wzorca.**

IV.
Nie dopuszcza się składania ofert częściowych.

V. Zamawiający zgodnie z art. 70^1 § 3 Kodeksu Cywilnego zastrzega sobie prawo zmiany lub odwołania ogłoszenia oraz warunków przetargu oraz zakończenia postępowania bez wyboru żadnej oferty.
Ponadto zamawiający zastrzega sobie prawo:

1. Żądania uzupełniania przez Wykonawcę złożonych ofert i załączonych do nich dokumentów, w terminie wyznaczonym przez Zamawiającego, jeśli, Wykonawca nie dostarczył wszystkich żądanych dokumentów czy informacji, dostarczył dokumenty lub informacje zawierające błędy, nieścisłości lub w dokumentach brak wszystkich informacji wymaganych przez Zamawiającego.
2. Żądania wyjaśnienia przez Wykonawcę złożonych ofert i załączonych dokumentów telefonicznie, pocztą elektroniczną lub za pomocą faksu, w terminie wyznaczonym przez Zamawiającego.
3. Żądania poprawienia złożonych ofert i załączonych do nich dokumentów o ile zawierają one błędy lub inne nieścisłości w terminie wyznaczonym przez Zamawiającego.

Oferty wykonawców, którzy w terminie wyznaczonym przez Zamawiającego:

a) nie uzupełnili złożonych ofert i załączonych do nich dokumentów,
b) nie wyjaśnili złożonych ofert lub załączonych do nich dokumentów,
c) nie poprawili złożonych ofert i załączonych do nich dokumentów,

oraz:
Oferty wykonawców, którzy nie wykazali (udowodnili) równoważności oferowanych przez siebie produktów w stosunku do wzorca.

nie będą rozpatrywane.

V. Termin wykonania zamówienia.

Wykonawca dostarczy licencje i zaktualizuje (zainstaluje i skonfiguruje w przypadku oferty równoważnej) oprogramowanie w terminie do 27.09.2022r. Jeżeli dostarczenie licencji i aktualizacja

(instalacja i konfiguracja w przypadku oferty równoważnej) oprogramowania nastąpi przed tą datą trzyletni okres ważności licencji oraz świadczenia usługi wsparcia liczony jest od 27.09.2022r.

VI. Osobami uprawnionymi do kontaktowania się z wykonawcami są:

W zakresie zagadnień technicznych:
Pani Agata Walter, e-mail: a.walter@pup.oswiecim.pl, 33 844-41-45 wew. 1202
W zakresie procedury:
Pan Ireneusz Drabik, i.drabik@pup.oswiecim.pl, 33 844-41-45 wew. 1209

VII. Opis sposobu przygotowania oferty.
Ofertę należy przesłać na adres e-mail: zp@pup.oswiecim.pl
lub pocztą tradycyjną (złożyć osobiście) na adres:
Powiatowy Urząd Pracy w Oświęcimiu
ul. Wyspiańskiego 10
32-600 Oświęcim
w terminie do 15.04.2022r. do godz. 9.00.

Wykonawcy są związani ofertą na okres 30 dni. Bieg 30-sto dniowego terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

VIII. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert.

1. Jedynym kryterium oceny ofert zastosowanym przez Zamawiającego jest **cena.**
2. Zamawiający udzieli zamówienia Wykonawcy, który zaoferuje najniższą cenę (zł brutto).

IX. Wzór umowy
§ 1
PRZEDMIOT UMOWY
1. Przedmiotem umowy jest …… według zamówienia PUP.
2. Wykonawca dostarczy licencje i zaktualizuje (zainstaluje i skonfiguruje w przypadku oferty równoważnej) oprogramowanie w terminie do 27.09.2022r. Jeżeli dostarczenie licencji i aktualizacja (instalacja i konfiguracja w przypadku oferty równoważnej) oprogramowania nastąpi przed tą datą trzyletni okres ważności licencji oraz świadczenia usługi wsparcia liczony jest od 27.09.2022r.
3. Szczegółowo opis przedmiotu zamówienia zawarty jest w warunkach przetargu oraz w ofercie wykonawcy, które to dokumenty stanowią załączniki do niniejszej umowy.
4. Wykonawca jest odpowiedzialny względem Zamawiającego za to, że jest uprawniony do wprowadzenia do obrotu licencji (oprogramowania) wymienionego w specyfikacji oraz za to, że Zamawiający wskutek zawarcia umowy będzie upoważniony do korzystania w ramach zwykłego użytku z tego oprogramowania.
5. W przypadku jeżeli realizacja zamówienia będzie wymagała dostępu do sprzętu, oprogramowania, danych itp. Zamawiającego Wykonawca zobowiązuje się do zawarcia z Zamawiającym odpowiedniej umowy z zakresu ochrony danych osobowych (RODO) w brzmieniu przedstawionym przez Zamawiającego.
6. Odmowa podpisania umowy w brzmieniu przedstawionym przez Zamawiającego będzie skutkowała odstąpieniem od umowy przez Zamawiającego z przyczyn, za które odpowiedzialność ponosi Wykonawca i naliczeniem kar umownych o których mowa w § 4 pkt 2 umowy.

§ 2

CENA I WARUNKI PŁATNOŚCI

1. Cena za przedmiot zamówienia jest zgodna z przedstawioną ofertą cenową.
2. Zamawiający zapłaci za dostawę przelewem po otrzymaniu rachunku.
3. Termin płatności określony w rachunku nie może być krótszy niż 14 dni.
4. Wykonawca oświadcza, że wypełnił i będzie wypełniał obowiązki informacyjne przewidziane w art. 13 lub art. 14 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) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał lub pozyska w celu zawarcia / wykonania niniejszej umowy. Klauzula informacyjna stanowi załącznik do niniejszej umowy.
5. Wykonawca będący płatnikiem podatku VAT zobowiązany jest do podania swojego nr rachunku bankowego na fakturze, który figuruje na liście podatników VAT, o której mowa w art. 96b ustawy z dnia 11 marca 2004r. o podatku od towarów i usług, pod rygorem wstrzymania płatności przez Zamawiającego. Przepis ten stosuje się odpowiednio do podwykonawcy oraz cesjonariusza.

§ 3

Wartość brutto dostarczonego towaru (usług) ustalona w dniu ..... w postępowaniu o udzielenie zamówienia publicznego wynosi: ..... zł, słownie: ..... złotych 00/100.

§ 4

1. Wykonawca zapłaci Zamawiającemu karę umowną za niedotrzymanie terminu wykonania zamówienia w wysokości 0,5 % wynagrodzenia umowy za każdy dzień zwłoki.
2. Wykonawca zapłaci Zamawiającemu karę umowną za odstąpienie od umowy przez Zamawiającego z przyczyn, za które odpowiedzialność ponosi Wykonawca w wysokości 20% wynagrodzenia umownego za przedmiot umowy.
3. Zamawiający zapłaci Wykonawcy karę umowną za odstąpienie od umowy przez Wykonawcę z przyczyn, za które ponosi odpowiedzialność Zamawiający w wysokości 20% wynagrodzenia umownego, poza przypadkiem, który określa ust. 4.
4. W razie wystąpienia 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. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.
5. Zamawiający ma prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższy wysokość kar umownych.

§ 5

Spory mogące wyniknąć z realizacji niniejszej umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.

§ 6

W sprawach nieuregulowanych niniejszą umową, mają zastosowanie odpowiednie przepisy Kodeksu Cywilnego.

§ 7

Umowę sporządzono w 2 jednobrzmiących egzemplarzach, tj. 1 egzemplarz dla Zamawiającego i 1 egzemplarz dla Wykonawcy.

X. Zgodnie z art. 13 ust. 1 i ust. 2 (art. 14) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

KLAUZULA INFORMACYJNA

(dla uczestników postępowań o udzielenie zamówienia publicznego, którego wartość nie przekracza 130 000 złotych)

Zgodnie z art. 13 ust. 1 i ust. 2, art. 14 ust. 1i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest Powiatowy Urząd Pracy w Oświęcimiu (PUP) – Dyrektor Powiatowego Urzędu Pracy w Oświęcimiu, ul. Wyspiańskiego 10, 32-602 Oświęcim (tel. 33 842 49 07, 33 842 57 71, 33 844 41 45; e-mail: poczta@pup.oswiecim.pl).
2. Inspektorem ochrony danych w Powiatowym Urzędzie Pracy w Oświęcimiu jest Pan Ireneusz Drabik (*e-mail: iod@pup.oswiecim.pl*).
3. Pani/Pana dane osobowe przetwarzane będą w celu związanym z postępowaniem o udzielenie zamówienia publicznego, którego wartość nie przekracza kwoty 130 000 złotych i do którego zgodnie z art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019r. – Prawo zamówień publicznych (t.j. Dz.U. z 2021r. poz. 1129 z późn. zm.) nie stosuje się w/w ustawy oraz art. 66 do 72 Kodeksu cywilnego lub/oraz w celu zawarcia i realizacji umowy zawartej z Panią/Panem tj.: zapewnienia obsługi techniczno – organizacyjnej Powiatowego Urzędu Pracy w Oświęcimiu, realizacji zamówienia publicznego (np. szkolenia, art. biurowe, wyposażenie, zasoby, media) na podstawie art. 6 ust 1 pkt „b" i „c" 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 osobowych (art. 6 ust. 1 pkt b - „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy"; art. 6 ust. 1 pkt c – „przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze").
4. Odbiorcą Pani/Pana danych osobowych będą inni uczestnicy postępowania o udzielenie zamówienia publicznego oraz mogą być inne podmioty upoważnione do ich przetwarzania na podstawie ustawy w szczególności, komornicy sądowi, sądy, policja, prokuratura.
5. Pani/Pana dane osobowe **nie będą** przekazywane do państwa trzeciego/organizacji międzynarodowej.
6. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów przetwarzania, jednak nie krócej niż przez czas określony przepisami prawa, w tym dla celów archiwalnych przez okres podyktowany ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w oparciu o Jednolity Rzeczowy Wykaz Akt obowiązujący w PUP.
7. Z zastrzeżeniem pkt 8 i 9 posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (*jeżeli przetwarzanie odbywa się na podstawie zgody*), którego dokonano na podstawie zgody przed jej cofnięciem.
8. Z prawa do bycia zapomnianym nie można skorzystać:
    a) w zakresie w jakim przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator danych (t.j.: prawa polskiego), lub do wykonania zadania realizowanego w interesie publicznych lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych.
    b) W zakresie w jakim przetwarzanie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa państwa członkowskiego (t.j.: prawa polskiego), jak również, jeżeli będzie to niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

9. Z prawa do przenoszenia danych nie można skorzystać do przetwarzania danych, które jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
10. Skorzystanie przez Pana / Panią, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 rozporządzenia 2016/679, nie może skutkować zmianą wyniku postępowania ani zmianą postanowień umowy w zakresie niezgodnym z przepisami obowiązującymi w tym zakresie.
11. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Dane adresowe:
    Urząd Ochrony Danych Osobowych
    ul. Stawki 2
    00-193 Warszawa
    fax. 22 531 03 01
12. Podanie przez Pana/Panią danych osobowych jest niezbędne do wykonania/zawarcia umowy oraz podjęcia działań na żądanie Pana/Pani, przed zawarciem umowy lub (i) podanie przez Pana/Panią danych osobowych jest wymogiem ustawowym. Jest Pan/Pani zobowiązana do ich podania. Konsekwencją niepodania danych osobowych będzie brak możliwości podjęcia na Pana/Pani żądanie działań, przed zawarciem umowy lub brak możliwości zawarcia/wykonania umowy lub(i) brak możliwości uczestniczenia w postepowaniu o udzielenie zamówienia publicznego.

KLAUZULA INFORMACYJNA
(dla osób reprezentujących, działających w imieniu lub na rzecz* przedsiębiorców, osób fizycznych i innych podmiotów w szczególności osób prawnych, jednostek organizacyjnych nie posiadających osobowości prawnej, jednostek sektora finansów publicznych w zakresie realizacji przez PUP w Oświęcimiu zamówień publicznych.

Zgodnie z art. 13 ust. 1 i ust. 2, art. 14 ust. 1i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest **Powiatowy Urząd Pracy w Oświęcimiu (PUP) – Dyrektor Powiatowego Urzędu Pracy w Oświęcimiu, ul. Wyspiańskiego 10, 32-602 Oświęcim** (tel. 33 842 49 07, 33 842 57 71, 33 844 41 45; e-mail: poczta@pup.oswiecim.pl)
2. Inspektorem ochrony danych w Powiatowym Urzędzie Pracy w Oświęcimiu jest Pan Ireneusz Drabik (*e-mail: iod@pup.oswiecim.pl*).
3. Pani/Pana dane osobowe przetwarzane będą w celu: związanym z postępowaniem o udzielenie zamówienia publicznego lub/oraz w celu zawarcia i realizacji umowy zawartej z podmiotem, który Pani / Pan reprezentuje lub działa w jego imieniu i na jego rzecz na podstawie art. 6 ust 1 pkt „c" i „e" 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 osobowych (art. 6 ust. 1 pkt. c – „przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze", art. 6 ust. 1 pkt e – „przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi") oraz w szczególności na podstawie Kodeksu cywilnego, Kodeksu spółek handlowych, przepisów regulujących zasady działania administracji publicznej.
4. Pani/Pana dane osobowe mogą być przekazane: innym uczestnikom postępowania o udzielenie zamówienia publicznego oraz mogą być również przekazywane innym podmiotom upoważnionym do ich przetwarzania na podstawie ustawy w szczególności, komornikom sądowym, sądom, policji, prokuraturze.

5. Pani/Pana dane osobowe **nie będą** przekazywane do państwa trzeciego/organizacji międzynarodowej.
6. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celów przetwarzania, w przypadku projektów unijnych zgodnie z warunkami umowy i przez czas przedawnienia ewentualnych roszczeń, jednak nie krócej niż przez czas określony przepisami prawa, w tym dla celów archiwalnych przez okres podyktowany ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w oparciu o Jednolity Rzeczowy Wykaz Akt obowiązujący w PUP w Oświęcimiu.
7. Z zastrzeżeniem pkt 8 i 9 posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (*jeżeli przetwarzanie odbywa się na podstawie zgody*), którego dokonano na podstawie zgody przed jej cofnięciem.
8. Z prawa do bycia zapomnianym nie można skorzystać:
   a) w zakresie w jakim przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator danych (t.j.: prawa polskiego), lub do wykonania zadania realizowanego w interesie publicznych lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych.
   b) w zakresie w jakim przetwarzanie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa państwa członkowskiego (t.j.: prawa polskiego), jak również, jeżeli będzie to niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
9. Z prawa do przenoszenia danych nie można skorzystać do przetwarzania danych, które jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
10. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Dane adresowe:
    Urząd Ochrony Danych Osobowych
    ul. Stawki 2
    00-193 Warszawa
    fax. 22 531 03 01
11. Podanie przez Pana/Panią danych osobowych jest wymogiem ustawowym i jednocześnie jest niezbędne do wykonania/zawarcia umowy z podmiotem który Pan/Pani reprezentuje, (działa w imieniu lub na rzecz). Jest Pan/Pani zobowiązana do ich podania w szczególności brak podania danych osobowych może spowodować brak możliwości rozpatrzenia wniosku, zawarcia lub realizacji umowy.

***W szczególności członków organów zarządzających, pełnomocników w tym prokurentów, osób reprezentujących jednostki sektora finansów publicznych na podstawie pełnomocnictw – upoważnień lub przepisów prawa.**

Załącznik Nr 1 do
warunków przetargu

....., dnia .....
(miejscowość)

Wykonawca:	
Nazwa Firmy:	
REGON:	
NIP:	
Adres Firmy:	
Nr telefonu:	
Nr faksu:	
e-mail:	

FORMULARZ OFERTOWY

Nawiązując do ogłoszenia dotyczącego postępowania o udzielenie zamówienia publicznego prowadzonego przez Powiatowy Urząd Pracy w Oświęcimiu oferujemy następującą cenę za przedmiot zamówienia:

L.p.	Wyszczególnienie	Ilość/ sztuk	Wartość (cena) netto	Wartość (cena) brutto
1.	Trzyletnia licencja na oprogramowanie antywirusowe …… …… …… z zapewnieniem w ramach licencji okresu bezpłatnego wsparcia w zakresie określonym w warunkach przetargu przez okres 3 lat (od 27.09.2022r.).	**100**		
Słownie złotych brutto:				

……
Podpisy osób uprawnionych do składania
oświadczeń woli w imieniu Wykonawcy