

## Warunki przetargu

Do niniejszego postępowania nie stosuje się Ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. z 2018r. poz. 1986 ze zm.) zgodnie z art. 4 pkt 8 w/w ustawy

### I. Nazwa i adres Zamawiającego

1. Zamawiający: Powiatowy Urząd Pracy w Oświęcimiu.
2. Adres: ul. Wyspiańskiego 10, 32-602 Oświęcim.

### II. Opis przedmiotu zamówienia: Zakup i dostawa licencji na oprogramowanie antywirusowe dla PUP. CPV – 48760000-3.

Zamówienie obejmuje zakup 100 licencji oprogramowania antywirusowego o parametrach i funkcjonalnościach opisanych poniżej, zapewnienie okresu wsparcia technicznego przez 36 miesięcy oraz startowe wdrożenie (instalacja, konfiguracja) do 10 punktów końcowych (stacji roboczych).

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.

#### Użyte rozwiązania i technologie:

- antimalware,
- antispymware,
- 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 mają być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem

4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony mają się łączyć klienci maszyn wirtualnych.
9. Integruje się 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 skrótów 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 rolę 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 poszukiwaniu 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 Cloud – serwer administracyjny po stronie producenta
- Konsola On-premise – 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 Cloud dostępna jest tylko 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 jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.

18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm.

19. W całym okresie trwania subskrypcji użytkownik ma 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 ma 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 :**

VMware vSphere 6.0, 5.5, 5.1, 5.0 P1 lub 4.1 P3

ESXi 4.1, 5.0, 5.1, 5.5

VMware vCenter Server 6.0, 5.5, 5.1, 5.0 or 4.1

VMware vShield Manager 5.5, 5.1, 5.0

VMware vShield Endpoint

VMware vCNS 5.5

VMware Tools 8.6.0 build 446312

VMware View 5.1, 5.0

Citrix XenDesktop 5.5, 5.0

Citrix XenServer 6.0, 5.6 or 5.5 w tym

Citrix Xen Hypervisor

Citrix VDI-in-a-Box 5.x

**Microsoft**

Microsoft Hyper-V Server 2012, 2008 R2 uwzględniając

Microsoft Hyper-V Hypervisor

### **Unix**

Red Hat Enterprise 3.0 w tym

Red Hat KVM Hypervisor

### **Oracle**

Oracle VM 3.0

### **Wspierane systemy operacyjne**

#### **System Operacyjny Windows:**

#### **Systemy Operacyjne Komputerów**

- Windows 10 Anniversary Update "Redstone"
- Windows 10 TH2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista z dodatkiem Service Pack 11
- Windows XP z Service Pack 2 64 bit1
- Windows XP z Service Pack 31

#### **Wbudowane Systemy Operacyjne**

- 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 Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP z wbudowanym Service Pack 2
- Windows XP Tablet PC Edition

#### **Systemy operacyjne serwera**

- Windows Server 2016
- Windows Server 2012 / Windows Server 2012 R2
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003/ Windows Server 2003 R21

Windows Server 2003/ Windows Server 2003 R21

- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 20081
- Windows Small Business Server (SBS) 20031
- Windows Home Server1

#### **Systemy Operacyjne Linux**

- Red Hat Enterprise Linux / CentOS 5.6 lub wyższy
- Ubuntu 14.04. lub wyższy
- SUSE Linux Enterprise Server 11 lub wyższy
- OpenSUSE 11 lub wyższy
- Fedora 16 lub wyższy
- Debian 7.0 lub wyższy
- Oracle Solaris 11, 10 (tylko w środowiskach VMware vShield)

- Oracle Linux 6.3 lub nowszy

#### **Systemy Operacyjne Mac OS X**

- Mac OS X Sierra (10.12.x)
- Mac OS X El Capitan (10.11.x)
- Mac OS X Yosemite (10.10.5)
- Mac OS X Mavericks (10.9.5)
- Mac OS X Mountain Lion (10.8.5)

#### **Obsługiwane Środowiska Microsoft Exchange**

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox
- Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG)

Dopuszcza się składanie ofert równoważnych. Za równoważną zamawiający uważa ofertę (produkt) posiadający parametry i funkcjonalności takie same lub wyższe (lepsze) niż wskazane powyżej w opisie przedmiotu zamówienia.

### **III.**

#### **Nie dopuszcza się składania ofert częściowych.**

V. Zamawiający zgodnie z art. 70<sup>1</sup> § 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,  
nie będą rozpatrywane.

#### **IV. Termin wykonania zamówienia.**

Zamówienie należy wykonać w terminie do 15 października 2019r.

**V. Osobami uprawnionymi do kontaktowania się z wykonawcami są:**

Pani Agata Walter, tel 8444145 wew. 1201 w zakresie zagadnień technicznych  
Pan Ireneusz Drabik, tel. 8444145 wew. 1209 w zakresie procedury  
w godz. od 7.30 do 14.00

**VI. Opis sposobu przygotowania oferty.**

**Ofertę należy przesłać na adres e-mail: [zp@pup.oswiecim.pl](mailto:zp@pup.oswiecim.pl)  
lub pocztą tradycyjną na adres:  
Powiatowy Urząd Pracy w Oświęcimiu  
ul. Wyspiańskiego 10  
32-600 Oświęcim  
w terminie do 20.09.2019r. 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.

**VII. 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).

**VIII. Wzór umowy**

**§ 1**

**PRZEDMIOT UMOWY**

1. Przedmiotem umowy jest ..... według zamówienia PUP.
2. Wykonawca zobowiązuje wykonać zamówienie w terminie do 15 października 2019r.
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. Wykonawca zapewni okres wsparcia dla oprogramowania wskazanego w pkt 1 na okres 36 miesięcy.
6. 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 (uwaga: dotyczy tylko czynnych podatników podatku VAT).
7. 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.

## § 2

### CENA I WARUNKI PŁATNOŚCI

1. Cena za ..... jest zgodna z przedstawioną ofertą cenową.
2. Zamawiający zapłaci za dostawę przelewem po wykonaniu zamówienia i otrzymaniu rachunku.
3. Termin płatności określony w rachunku nie może być krótszy niż 14 dni.

## § 3

Wartość brutto zamówienia 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 niezapewnienie wsparcia w okresie o którym mowa w § 1 pkt 5 w wysokości 0,5 % wynagrodzenia umowy za każdy dzień braku wsparcia.
3. 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.
4. 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. 5.
5. 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.
6. 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 nie uregulowanych niniejszą umową, mają zastosowanie odpowiednie przepisy Kodeksu Cywilnego.

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



## KLAUZULA INFORMACYJNA

### (dla uczestników postępowań o udzielenie zamówienia publicznego prowadzonych na podstawie art. 4 pkt 8 ustawy Prawo zamówień publicznych)

Zgodnie z art. 13 ust. 1 i 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 44; 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 prowadzonym zgodnie z art. 4 pkt 8 ustawy z dnia 29 stycznia 2004r. – Prawo zamówień publicznych (Dz.U. z 2018r. poz. 1986 z późn. zm.) 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 postępowaniu 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 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 44; 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:
  - c) 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.
  - d) 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 składania ofert

....., dnia .....

(miejsowość)

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

**FORMULARZ OFERTOWY**

Nawiązując do ogłoszenia dotyczącego postępowania o udzielenie zamówienia publicznego oferujemy następującą cenę za przedmiot zamówienia:

L.p.	Wyszczególnienie	Ilość sztuk (licencji)	Wartość (cena) netto	Wartość (cena) brutto
1.	Licencje na oprogramowanie antywirusowe ..... ..... ..... z zapewnieniem w ramach licencji okresu bezpłatnego wsparcia w zakresie określonym w warunkach przetargu przez okres 36 miesięcy oraz startowe wdrożenie (instalacja, konfiguracja) do 10 punktów końcowych (stacji roboczych).	<b>100</b>		
<b>Słownie złotych brutto:</b>				

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