ZATWIERDZAM

Grzegorz Mroczek

Dyrektor Działu Bezpieczeństwa

/podpisano elektronicznie/

Warszawa, dnia 1 kwietnia 2021 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

(SWZ)

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP.

Nr postępowania 16/21/TPBN

<u>TRYB UDZIELENIA ZAMÓWIENIA</u>:

tryb podstawowy bez negocjacji

Zamawiający oczekuje, że Wykonawcy zapoznają się dokładnie z treścią niniejszej SWZ. Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów, oraz przedłożenia oferty nie odpowiadającej wymaganiom określonym przez Zamawiającego.

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO ORAZ WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI:

1. Zamawiający: NARODOWE CENTRUM BADAŃ I ROZWOJU W WARSZAWIE ul. Nowogrodzka 47a, 00-695 Warszawa.

   Numer tel.: 22 390 73 58

   Adres poczty elektronicznej: przetargi@ncbr.gov.pl.

   Adres strony internetowej prowadzonego postępowania: https://www.gov.pl/web/ncbr/postepowania-rozpoczete.

   Składanie ofert poprzez stronę: https://miniportal.uzp.gov.pl/

2. Wskazanie osób uprawnionych do komunikowania się z wykonawcami:

   Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:

   Imię Nazwisko: Jakub Wojtkowski

   e-mail: przetargi@ncbr.gov.pl

II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: https://www.gov.pl/web/ncbr/postepowania-rozpoczete.

III. TRYB UDZIELENIA ZAMÓWIENIA

1. Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie **art. 275 pkt 1** ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 ze zm.) [zwanej dalej także „ ustawą PZP" lub „uPzp].
2. W zakresie nieuregulowanym niniejszą Specyfikacją Warunków Zamówienia, zwaną dalej „SWZ”, zastosowanie mają przepisy ustawy PZP.

IV. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

V. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa systemu klasy DLP z licencjami, wraz ze wsparciem, na okres 24 miesięcy dla 800 stanowisk. Szczegółowy opis przedmiotu zamówienia (SOPZ) znajduje się w Załączniku nr 1 do niniejszej Specyfikacji Warunków Zamówienia (SWZ) i stanowi jej integralną część.

2. Zamawiający przewiduje prawo opcji w zakresie dostawy licencji do zaoferowanego systemu dla maksymalnie 160 stanowisk. Okres wsparcia i ważności licencji musi być zrównany z okresem wsparcia i ważności licencji dostarczonym w ramach zamówienia podstawowego.
3. Zamawiający nie dopuszcza składania ofert częściowych.
4. Zamawiający nie dopuszcza możliwości składania ofert wariantowych oraz w postaci katalogów elektronicznych.
5. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8.
6. Zamawiający nie wymaga, aby osoby wykonujące czynności w zakresie realizacji zamówienia zostały zatrudnione na podstawie umów o pracę.
7. Zamówienie jest niepodzielne. Ze względów technologicznych i wykonawczych oraz racjonalnego wydatkowania środków publicznych nie ma możliwości podzielenia go na części. Podział tego zamówienia groziłby zakupem więcej niż jednego systemu pełniącego taką samą funkcję, co jest niedopuszczalne z punktu widzenia bezpieczeństwa. Zamawiający zrobił rozeznanie rynku i tego typu zamówieniami zajmują się wyspecjalizowani w tym kierunku Wykonawcy. Nie dzielenie zamówienia na części nie wyklucza udziału w tym postępowaniu wykonawców z MŚP.
8. Nazwy i kody zamówienia według Wspólnego Słownika Zamówień (CPV):

   48000000-8 Pakiety oprogramowania i systemy informatyczne

VI. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie 24 miesięcy od dnia podpisania umowy, w tym:

-dostawa licencji – 10[1] dni roboczych od dnia zawarcia umowy;

-przeprowadzenie szkolenia – 90 dni od dnia podpisania bez uwag protokołu odbioru.

VII. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają określone przez Zamawiającego w niniejszym rozdziale warunki udziału w postępowaniu dotyczące:

   1.1. zdolności technicznej lub zawodowej.
2. W zakresie warunku określonego w art. 112 ust. 2 pkt 4) ustawy PZP (zdolności technicznej lub zawodowej), Wykonawcy winni wykazać że:

   2.1 w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie co najmniej dwie dostawy systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention), dla co

[1] Lub krócej, zgodnie z ofertą Wykonawcy

najmniej 400 stanowisk każda i o wartości zamówienia co najmniej 100 000 zł brutto każda.

Na potwierdzenie spełnienia ww. warunków Wykonawcy przedłożą oświadczenie wymienione w pkt 12 SWZ oraz - na wezwanie, oświadczenie i dokumenty, o których mowa w rozdziale XII pkt 20 SWZ. W przypadku, gdy Wykonawcy będą polegać na zdolnościach technicznych lub zawodowych innego podmiotu, o którym mowa w art. 118 ust. 1 ustawy PZP, Wykonawca wraz z ofertą składa także oświadczenie tego podmiotu, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu lub kryteriów selekcji, w zakresie, w jakim wykonawca powołuje się na jego zasoby.

3. W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o wykonanie zamówienia wystarczy, że ww. warunki spełni jeden z nich lub Wykonawcy spełnią go łącznie.
4. Ocena spełnienia ww. warunków odbywać się będzie metodą spełnia/nie spełnia.
5. Z treści załączonych dokumentów i oświadczeń musi wynikać jednoznacznie, iż Wykonawca spełnia wyżej wymienione warunki.
6. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.
7. Niespełnienie warunku skutkować będzie odrzuceniem oferty Wykonawcy z postępowania.
8. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
9. W takim przypadku:
   9.1. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
   9.2. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 9.1. potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
      1) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;

2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;

3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje dostawy, których wskazane zdolności dotyczą.

10. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, o których mowa w art. 112 ust. 2 pkt 4.
11. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają dostawy, do realizacji których te zdolności są wymagane.
12. W celu potwierdzenia spełniania warunków udziału w postępowaniu oraz wykazania braku podstaw wykluczenia, określonych w rozdziale XV, Wykonawcy ubiegający się o udzielenie zamówienia muszą wraz z ofertą złożyć następujące dokumenty:
    12.1. aktualne na dzień składania ofert oświadczenie o niepodleganiu wykluczeniu z postępowania w zakresie wskazanym odpowiednio w Załączniku nr 3 do SWZ. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu.
    12.2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym mowa w pkt 11.1. SWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to potwierdza brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców brak podstaw wykluczenia.

VIII PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści umowy, określone zostały w Załączniku nr 4 do SWZ.

IX. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną przy użyciu miniPortalu https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal.
2. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do *formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.*
3. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej przekazywanej przy ich użyciu, opisane zostały w Regulaminie korzystania z miniPortalu dostępnym pod adresem https://miniportal.uzp.gov.pl/WarunkiUslugi.aspx oraz Regulaminie ePUAP.
4. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z miniPortalu, określone w Regulaminie miniPortalu oraz zobowiązuje się korzystając z miniPortalu przestrzegać postanowień tego regulaminu.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia i wycofania oferty oraz do komunikacji wynosi 150 MB.
6. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 ustawy pzp, podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na ePUAP.
7. W postępowaniu o udzielenie zamówienia korespondencja elektroniczna (inna niż oferta Wykonawcy i załączniki do oferty) odbywa się elektronicznie za pośrednictwem *dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji).* Korespondencja przesłana za pomocą tego formularza nie może być szyfrowana. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP).
8. Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, email: przetargi@ncbr.gov.pl
9. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem *Formularza do komunikacji,* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na adres email przetargi@ncbr.gov.pl. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 31 grudnia 2020 roku „*W sprawie sposobu sporządzania i przekazywania informacji oraz wymagań*

technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie".

10. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
11. Zamawiający nie ponosi odpowiedzialności z tytułu nieotrzymania przez Wykonawcę informacji związanych z prowadzonym postępowaniem w przypadku wskazania przez Wykonawcę w ofercie np. adresu poczty elektronicznej.
12. Wykonawca może w drogą elektroniczną/za pomocą środków komunikacji elektronicznej zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający niezwłocznie udzieli wyjaśnień jednak nie później niż **2 dni** przed terminem składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego nie później niż na 4 dni przed upływem wyznaczonego terminu składania ofert i nie dotyczy udzielonych wyjaśnień.
13. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania ww. wniosków. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął po upływie terminu, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
14. Wnioski o wyjaśnienia SWZ należy przesyłać za pomocą poczty elektronicznej na adres: przetargi@ncbr.gov.pl. W temacie pisma należy podać ***„Nr 16/21/TPBN dostawa systemu ochrony przed wyciekiem informacji DLP”.***
15. Treść zapytań wraz z wyjaśnieniami Zamawiający przekaże Wykonawcy oraz zamieści na stronie internetowej prowadzonego postępowania bez ujawniania źródła zapytania.
16. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert zmodyfikować treść niniejszej SWZ.
17. Każda wprowadzona przez Zamawiającego zmiana SIWZ stanie się częścią SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej Zamawiającego.
18. Zamawiający przedłuży termin składania ofert, jeżeli w wyniku modyfikacji treści SWZ niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach.

X. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert przez 30 (trzydzieści) dni kalendarzowych tj. do dnia 08.05.2021 r.
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w SWZ, Zamawiający przed upływem terminu związania oferta zwróci się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.

3. Przedłużenie terminu związania oferta, o którym mowa w pkt 1 wymaga złożenia przez Wykonawcę pisemnego[2] oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. **Oferta musi być** sporządzona w języku polskim, w postaci elektronicznej w formacie danych: .pdf, .doc, .docx, .rtf,.xps, .odt i **opatrzona kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.**
2. Sposób zaszyfrowania oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
3. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego lub podpisu zaufanego lub podpisu osobistego.
4. Jeżeli na ofertę składa się kilka dokumentów, Wykonawca powinien stworzyć folder, do którego przeniesie wszystkie dokumenty oferty, podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Następnie z tego folderu Wykonawca skompresuje do jednego folderu .zip.
5. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj.: Dz. U. z 2020 r. poz. 1013), które Wykonawca zastrzeże, jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego, jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 pzp.

   Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Zaleca się, aby uzasadnienie, o którym mowa powyżej było sformułowane w sposób umożliwiający jego udostępnienie inny uczestnikom postępowania.

   Uwaga:

   Zastrzegając informacje w ofercie Wykonawca winien mieć na względzie, że zastrzeżona informacja ma charakter tajemnicy przedsiębiorstwa, jeśli spełnia poniższe warunki, określone w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji tj.:

[2] *t.j. wyrażonego przy użyciu wyrazów, cyfr lub innych znaków pisarskich, które można odczytać i powielić*

ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą, ***oraz***

jako całość lub w szczególnym zestawieniu i zbiorze elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji, ***albo*** *nie są łatwo dostępne dla takich osób,*

o ile uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

W nawiązaniu do orzecznictwa arbitrażowego i sądowego, należy przyjąć, iż sferą tajemnicy można objąć tylko takie informacje, które są znane jedynie poszczególnym osobom lub określonej grupie osób. Obszar ten nie może się rozciągać na informacje powszechnie znane lub te, o których treści każdy zainteresowany może się legalnie dowiedzieć.

6. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnym pliku oznaczonym, jako tajemnica przedsiębiorstwa. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
7. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 224 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich, jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
8. Wykonawca w szczególności nie może zastrzec w ofercie informacji:
   8.1 Przekazywanych po otwarciu ofert, o których mowa w art. 222 ust. 5 ustawy PZP,
   8.2 które są jawne na mocy odrębnych przepisów,
   8.3 cen jednostkowych stanowiących podstawę wyliczenia ceny oferty.
9. Wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania powyższych wymagań będą obciążały Wykonawcę.
10. Do oferty należy dołączyć wstępne oświadczenie o spełnieniu warunków udziału i niepodleganiu wykluczeniu w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
11. Do przygotowania oferty zaleca się wykorzystanie Formularza oferty, którego wzór stanowi Załącznik nr 2 do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu oferty.
12. Miniportal oraz ePuap nie weryfikuje poprawności podpisu z profilu zaufanego oraz podpisu osobistego, jak również nie weryfikuje poprawności dokumentów, poprawności rozumianej zgodnej w ustawą PZP i kompletności zgodnego z SWZ.

13. **<u>Do oferty należy dołączyć:</u>**

13.1 **Pełnomocnictwo upoważniające do złożenia oferty** - o ile ofertę składa pełnomocnik (podpisane zgodnie z informacją zawartą w pkt 16).

13.2 **Formularz oferty –** do wykorzystania wzór, stanowiący Załącznik nr 2 do SWZ (podpisany kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym).

13.3 **Wstępne oświadczenie Wykonawcy o niepodleganiu wykluczeniu z postępowania** wzór wstępnego oświadczenia o niepodleganiu wykluczeniu stanowi Załącznik nr 3 do SWZ. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepoleganiu wykluczeniu składa każdy z Wykonawców (podpisany kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym).

13.4 **Zobowiązanie podmiotu trzeciego –** jeżeli dotyczy (podpisane zgodnie z informacją zawartą w pkt 17).

13.5

13.6 **Oświadczenie, o którym mowa w art. 117 ust. 4 –** w przypadku wykonawców wspólnie ubiegających się o zamówienie – do wykorzystania wzór, stanowiący Załącznik nr 8 (podpisany kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym).

14. Ofertę, oświadczenia zaleca się sporządzić na drukach stanowiących załączniki do SWZ.

15. Oferta, wstępne oświadczenie o spełnieniu warunków udziału i niepodleganiu wykluczeniu oraz oświadczenie, o którym mowa w art. 117 ust. 4 muszą być złożone w oryginale.

16. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym. Zamawiający dopuszcza również skan pełnomocnictwa sporządzonego uprzednio w formie opatrzony pisemnej kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

17. **Wykonawcy ubiegający się wspólnie o udzielenie zamówienia** (np. spółki cywilne, konsorcja), zgodnie z art. 58 ust. 2 ustawy PZP, **<u>zobowiązani są ustanowić pełnomocnika.</u>** Z treści pełnomocnictwa winno jednoznacznie wynikać prawo pełnomocnika do reprezentowania Wykonawcy w postępowaniu o udzielenie zamówienia publicznego albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego w imieniu Wykonawcy. Dokument ten winien być podpisany przez osobę/osoby uprawnioną(-e) do jego udzielenia tj. zgodnie z formą reprezentacji każdego z Wykonawców (podpisany kwalifikowanym podpisem elektronicznym lub profilem zaufanym lub podpisem osobistym). W przypadku wspólników spółki

cywilnej dopuszczalne jest przedłożenie umowy spółki cywilnej, z której wynika zakres i sposób reprezentacji, a w przypadku konsorcjum przedłożenie umowy konsorcjum.

18. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
19. Postanowień pkt 18 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzaniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
20. Zgodnie z art. 274 ust. 1 ustawy Pzp, zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych, o których mowa w art. 273 ust. 1 ustawy PZP:

    21.1. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;

    21.2. Wykaz dostaw wykonanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem przedmiotu dostawy, dat wykonania, nazwy podmiotu na rzecz, którego była realizowana dostawa oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, że zostały wykonane należycie. Do ewentualnego wykorzystania przy sporządzaniu tego dokumentu służy Załącznik nr 9 do SWZ
22. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej zamiast: odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury

23. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 21, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 ustawy Pzp zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy.
24. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
25. Wykonawca składa podmiotowe środki dowodowe aktualne na dzień ich złożenia.
26. W przypadku, kiedy Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcy, Zamawiający żąda wskazania przez wykonawcę w Formularzu oferty, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez wykonawcę firm podwykonawców o ile są znane.

XIII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia lub wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia 09.04.2021 r., do godz. 14.00.
3. Wykonawca może złożyć tylko jedną ofertę.
4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
5. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
6. Wykonawca po przesłaniu oferty za pomocą Formularza do złożenia lub wycofania oferty na „ekranie sukcesu" otrzyma numer oferty generowany przez ePUAP. Ten numer należy zapisać i zachować. Będzie on potrzebny w razie ewentualnego wycofania oferty.
7. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem Formularza do wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
8. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

XIV. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu 12.04.2021 r. o godzinie 11:00
2. Otwarcie ofert jest niejawne.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informacją o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

4. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
   4.1. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   4.2. cenach lub kosztach zawartych w ofertach.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
7. W toku dokonywania badania i oceny złożonych ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących ich treści.
8. Oferty, które nie zostaną odrzucone, zostaną poddane procedurze oceny zgodnie z kryterium oceny ofert określonym w rozdziale XVIII niniejszej SWZ.
9. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie PZP oraz w SWZ, a ponadto uzyska największą liczbę punktów zgodnie z przyjętym kryterium oceny ofert.

XV. PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia wyklucza się z zastrzeżeniem art. 110 ust. 2 ustawy PZP, Wykonawcę w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych;
   1.1. w art. 108 ust.1 ustawy PZP;
   1.2. w art. 109 ust. 1 pkt 4, 5, 7 ustawy PZP, tj.:
      a. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
      b. który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;
      c. który z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;
   1.3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 ustawy PZP.

XVI. SPOSÓB OBLICZENIA CENY

1. Wykonawca poda cenę oferty w Formularzu oferty sporządzonym według wzoru stanowiącego Załącznik nr 2 do SWZ, tj. cenę netto, cenę brutto (z uwzględnieniem kwoty podatku od towarów i usług (VAT) z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku.
3. Wykonawca poda w Formularzu oferty stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty.
4. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
5. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.

XVII. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Za najkorzystniejszą zostanie uznana oferta z największą ilością punktów.
2. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty dwie lub więcej ofert przedstawiających taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający zastosuje procedurę opisaną w art. 248 ustawy PZP.
3. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
4. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższa oceną, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
5. W przypadku braku zgody, o której mowa w ust. 4, oferta podlega odrzuceniu, a Zamawiający zwróci się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba ze zachodzą przesłanki do unieważnienia postępowania.
6. Zamawiający dokona oceny ofert, które nie będą podlegały odrzuceniu. **Przy ocenie ofert zostaną uwzględnione następujące kryteria:**

   6.1. Kryterium cena oferty brutto – waga kryterium 60%;

   6.2. Termin realizacji zamówienia (dostarczenia licencji) – waga kryterium 20%

   6.3. Stawka za 1 roboczogodzinę usług wsparcia technicznego i serwisu – waga kryterium 20%
7. Zamawiający oceni oferty przyznając punkty w ramach kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt. Zamawiający dokona wyliczenia punktów dla danej oferty do dwóch miejsc po przecinku i wybierze ofertę z najwyższą liczbą punktów ogółem, spośród ofert nie podlegających odrzuceniu.

8. **Punkty za kryterium: cena oferty brutto „CO" – waga 60%**

Maksymalną liczbę punktów w tym kryterium (60 pkt) otrzyma oferta Wykonawcy, który zaproponuje najniższą cenę oferty brutto, z wyłączeniem wartości usługi wsparcia technicznego i serwisu rozliczanego w roboczogodzinach, podaną przez Wykonawcę w Formularzu oferty (Załącznik nr 2 do SWZ), natomiast pozostali Wykonawcy otrzymają odpowiednio mniejszą liczbę punktów obliczoną zgodnie z poniższym wzorem:

$$\textbf{CO}\ (\text{liczba przyznanych punktów}) = \frac{\text{cena brutto oferty najtańszej}}{\text{cena brutto oferty badanej}} \times 60$$

Punkty w kryterium „**Cena oferty brutto**" zostaną zaokrąglone do dwóch miejsc po przecinku.

Wykonawca za kryterium „**Cena oferty brutto**" może uzyskać maksymalnie 60 pkt.

9. **Punkty za kryterium: Termin realizacji zamówienia „T" – waga 20%**

Maksymalną liczbę punktów w tym kryterium (20 pkt) otrzyma oferta Wykonawcy, który zaproponuje najkrótszy termin realizacji (dostarczenia licencji) podany przez Wykonawcę w Formularzu oferty (Załącznik nr 2 do SWZ), natomiast pozostali Wykonawcy otrzymają odpowiednio mniejszą liczbę punktów obliczoną zgodnie z poniższym wzorem:

$$\textbf{T}\ (\text{liczba przyznanych punktów}) = \frac{\text{Najkrótszy termin realizacji}}{\text{Termin realizacji oferty badanej}} \times 20$$

Punkty w kryterium „**Termin realizacji zamówienia**" zostaną zaokrąglone do dwóch miejsc po przecinku.

Wykonawca za kryterium „**Termin realizacji zamówienia**" może uzyskać maksymalnie 20 pkt.

10. **Punkty za kryterium: stawka za 1 roboczogodzinę usług wsparcia technicznego i serwisu „RB" – waga 20%**

Maksymalną liczbę punktów w tym kryterium (20 pkt) otrzyma oferta Wykonawcy, który zaproponuje najniższą cenę brutto za roboczogodzinę usług wsparcia technicznego i serwisu podaną przez Wykonawcę w Formularzu oferty (Załącznik nr 2 do SWZ), natomiast pozostali Wykonawcy otrzymają odpowiednio mniejszą liczbę punktów obliczoną zgodnie z poniższym wzorem:

$$\textbf{RB}\ (\text{liczba przyznanych punktów}) = \frac{\text{Najniższa stawka za roboczogodzinę}}{\text{Stawka za roboczogodzinę oferty badanej}} \times 20$$

Punkty w kryterium „**stawka za 1 roboczogodzinę usług wsparcia technicznego i serwisu**" zostaną zaokrąglone do dwóch miejsc po przecinku.

Wykonawca za kryterium „**stawka za 1 roboczogodzinę usług wsparcia technicznego i serwisu**” może uzyskać maksymalnie 20 pkt.

11. Po ocenie ofert, o której mowa powyżej, poszczególne oferty otrzymują ilość punktów wyliczoną według poniższej formuły:

    OO = CO + T + RB

    Gdzie:

    OO - oznacza ilość punktów przyznanych ocenianej ofercie;

    CO - oznacza ilość punktów przyznanych ocenianej ofercie za kryterium cena;

    T – oznacza ilość punktów przyznanych ocenianej ofercie za kryterium termin realizacji zamówienia

    RB - oznacza ilość punktów przyznanych ocenianej ofercie za kryterium stawka za 1 roboczogodzinę usług wsparcia technicznego i serwisu

12. Zamawiający odrzuci ofertę w sytuacjach, o których mowa w art. 226 ust. 1 ustawy Pzp.

XVIII. POPRAWIENIE OMYŁEK W OFERCIE

1. Zamawiający poprawi w ofercie, w szczególności:
   1.1. oczywiste omyłki pisarskie;
   1.2. oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek;
   1.3. inne omyłki - polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty.

   - poprawieniu omyłek w ofercie Zamawiający niezwłocznie zawiadomi Wykonawcę, którego oferta została poprawiona.

2. W przypadku, o którym mowa w ust. 1 pkt 3 powyżej, Zamawiający wyznaczy Wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki.

XIX. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 ustawy PZP w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umową w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w pkt 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.

3. Wykonawca, którego oferta została wybrana, jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią Załącznik nr 4 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty, jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana, jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego. Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

XX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów pzp.
2. Odwołanie przysługuje na:
   2.1. niezgodną z przepisami ustawy czynność Zamawiającego, podjęta w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy PZP, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargą wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" ustawy PZP.

XXI. ZAŁĄCZNIKI DO SWZ

Integralną częścią niniejszej SWZ stanowią następujące załączniki:

Załącznik nr 1- Szczegółowy opis przedmiotu zamówienia;

Załącznik nr 2- Formularz oferty;

Załącznik nr 3- Wstępne oświadczenie o niepodleganiu wykluczeniu;

Załącznik nr 4- Projektowane postanowienia umowy;

Załącznik nr 5- Regulamin korzystania z miniPortalu.

Załącznik nr 6- Arkusz weryfikacji podmiotu przetwarzającego dane osobowe;

Załącznik nr 7- Klauzula informacyjna dotycząca przetwarzania danych osobowych;

Załącznik nr 8 – Oświadczenie, o którym mowa w art. 117 ust. 4,

Załącznik nr 9 – wzór wykazu dostaw.

Załącznik nr 1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention), wraz z kompletem niezbędnych licencji, przeszkoleniem pracowników oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu.

SŁOWNIK POJĘĆ

Tag – Oznaczenie stosowane na plikach i dokumentach elektronicznych, wiadomościach mailowych umożliwiające identyfikację. Tag może istnieć: w treści dodanej w metadanych, w postaci nagłówka, stopki lub dodatkowego elementu np. pliku JPEG dodanego do pliku;

Klasyfikacja dokumentów / plików – Nadawanie odpowiedniej kategorii. Kategorie są możliwe do zdefiniowania i edycji np. poufne, tajne. Możliwość nadawania poprzez odpowiedni system lub funkcję np. menu kontekstowe w systemie Windows;

Polityka – inaczej zasada DLP to pakiet stanowiący zbiór reguł, które zawierają określone warunki, akcje i wyjątki, które mogą np. monitorować pliki na podstawie ich zawartości i generować incydenty.

1. **W ramach realizacji przedmiotu zamówienia mieści się:**
   - 1.1 Dostawa niezbędnych licencji i oprogramowania oferowanego systemu DLP dla 800 stanowisk w ramach zamówienia podstawowego, na okres 24 miesięcy;
   - 1.2 Zamawiający zastrzega sobie możliwość zakupu w ramach prawa opcji 20% dodatkowych licencji, ujętych w zamówieniu podstawowym pkt 1.1., w razie zaistnienia potrzeby, w terminie obowiązywania umowy;
   - 1.3 Świadczenie serwisu i wsparcia technicznego wykonawcy (punkt 4) przez okres obowiązywania umowy;
   - 1.4 Gwarancja Producenta elementów oprogramowania świadczona przez okres obowiązywania Umowy;

1.5 Przeprowadzenie szkolenia z zakresu administracji zamawianego oprogramowania, dla min. 4 osób, w terminie do 90 dni kalendarzowych od dnia podpisania bez uwag protokołu odbioru;

2. Wymagania dotyczące dostawy oprogramowania oraz licencji:

2.1 Dostawa musi zostać zrealizowana zgodnie z terminem wskazanym w ofercie Wykonawcy, ale nie później niż 10 dni roboczych od dnia podpisania umowy;

2.2 Wykonawca zobowiązuje się dostarczyć wymagane, oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta. Pomoc serwisowa musi być świadczona w języku polskim.

2.3 Dostawa oprogramowania, aplikacji, modułów, wymaganych do prawidłowego funkcjonowania zaoferowanego systemu DLP, zgodnie z wymaganymi funkcjonalnościami oraz specyfikacją Zamawiającego;

2.4 Dostawa licencji wymaganych do poprawnej pracy systemu DLP, zgodnie z wymaganymi funkcjonalnościami opisanymi w specyfikacji;

2.5 Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików.

3. Wymagania dot. oprogramowania DLP

3.1.Zamawiający wymaga dostarczenia oprogramowania, zapewniającego ochronę przed wyciekiem poufnych danych (ang. Data Loss Prevention - DLP) obejmującego:

3.1.1. Ochronę stacji końcowych użytkowników Zamawiającego;

3.1.2. Ochronę i monitoring danych przesyłanych za pośrednictwem sieci LAN i/lub WAN;

3.1.3. Ochronę danych przesyłanych za pośrednictwem kanału drukowania (np. protokół LPD, IPP);

3.1.4. Ochronę danych przesyłanych za pośrednictwem kanału komunikacyjnego poczty email Zamawiającego (np. protokół SMTP, SMPTS);

3.1.5. Monitorowanie bezpieczeństwa plików aktualnie używanych np. zapisanych tymczasowo w pamięci podręcznej, otwartych w edytorze tekstu;

3.1.6. Monitorowanie i ochronę zasobów plikowych Zamawiającego np. baz danych, plików współdzielonych, archiwów cyfrowych i elektronicznego obiegu dokumentów;

3.1.7. Wielopoziomową klasyfikację dokumentów (tj. dodawanie dynamicznych nagłówków plików, dodawanie informacji o ważności pliku) Klasyfikacja jest widoczna dla użytkowników i systemów i podąża razem z plikiem;

3.1.8. Monitorować przepływ danych usług zdalnego pulpitu, zdalnego dostępu i udostępniania ekranu (np. RDP, VNC, SSH) wraz z wywoływaniem określonych akcji, zgodnie z przyjętymi politykami, w zależności od rodzaju przesyłanych treści;

3.2. **Podstawowe funkcje oprogramowania DLP**

Zamawiane oprogramowanie musi:

3.2.1. Być typu „End-Point" (serwer zarządzający/konsola zarządzająca + końcówki klienckie);

3.2.2. Umożliwiać przeglądanie zaistniałych zgłoszeń poprzez konsolę zarządzającą;

3.2.3. Umożliwiać definiowanie polityki ochrony przed wyciekiem np. na stacjach końcowych, poprzez pojedynczy punkt konfiguracji (konsola zarządzająca);

3.2.4. Umożliwiać definiowanie określonych akcji (przynajmniej blokowanie, monitorowanie, wysłanie komunikatu do użytkownika i/lub administratora Systemu DLP) następujących w przypadku wykrycia zagrożenia wycieku danych, w zależności od kanału komunikacyjnego, którego zagrożenie dotyczy;

3.2.5. Zapewniać, aby zasady tworzenia polityk bezpieczeństwa umożliwiały budowę polityki w oparciu o co najmniej następujące dane wprowadzane do tej polityki: zdefiniowaną zawartość podlegająca wykryciu, odbiorcę, nadawcę, rodzaje plików, rodzaje kanałów komunikacyjnych (np. protokoły HTTPS, SMPT), dane użytkownika końcowego jak: nazwy stacji końcowej użytkownika;

3.2.6. Umożliwiać nadawanie określonych poziomów ważności zdarzeń dotyczących wycieku danych;

3.2.7. Wspierać co najmniej uwierzytelnianie użytkowników w modelu użytkownik, grupa, rola (ang. model RBAC) oraz integrację z repozytorium danych Microsoft Active Directory, z uwzględnieniem możliwości wykorzystania struktury danych w nim zawartych (np. działy, grupy, lokalizacje);
3.2.8. Umożliwiać przeprowadzenie audytu stacji końcowych w oparciu o: uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, pliki wysłane do drukowania, ruch sieciowy, wysłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach;
3.2.9. Umożliwiać stosowanie gotowych algorytmów detekcji, wykrywających pojawienie się ustalonego wzorca (np. PESEL) (działających tam gdzie to możliwe o mechanizm sum kontrolnych w celu walidacji danych);
3.2.10. Umożliwiać zarządzanie ilością i retencją przechowywanych danych, obejmując dane całego systemu jak i dane dotyczące pojedynczych zdarzeń (w tym incydentów);
3.2.11. Zapewniać konsolę zarządczą oprogramowania, która jest dostępna przez przeglądarkę internetową (Web) z możliwością użycia przeglądarek wiodących dostawców, takich jak co najmniej dwie z podanych: Microsoft (egde), Google (Chrome), Mozilla (Firefox);
3.2.12. Umożliwiać integrację z innymi rozwiązaniami bezpieczeństwa używanymi u Zamawiającego tj.: system SIEM (Splunk), poprzez automatyczne raportowanie incydentów, NGFW (Fortigate) oraz system antyspam (Fortimail), celem zachowania automatyzacji środowiska Zamawiającego;
3.2.13. Musi posiadać własny klasyfikator, umożliwiający klasyfikację informacji, którą może prowadzić zarówno administrator i użytkownik systemu na stacji końcowej;
3.2.14. Umożliwiać integrację z systemami wspierającymi zarządzanie stacjami roboczymi (w szczególności Microsoft SCCM wykorzystywanym u Zamawiającego) w zakresie dystrybucji i zarządzania konfiguracją oprogramowania na końcówkach klienckich, a także posiadać instalatory w formatach msi lub exe (dmg/pkg); Zamawiający planuje dystrybucję oferowanego oprogramowania za pomocą oprogramowania Microsoft SCCM.
3.2.15. Stanowić jednolity produkt, najlepiej zarządzany pojedynczą konsolą zarządczą z dodatkową konsolą webową, działający bez konieczności

używania zewnętrznych modułów administracyjnych firm trzecich, z wykorzystaniem oprogramowania zainstalowanego na serwerze;

3.2.16. Posiadać konsolę webową, która umożliwia przeglądanie informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików pobieranych i wysyłanych za pośrednictwem protokołów sieciowych (TCP oraz UDP), zarówno w obrębie sieci LAN, jak i sieci WAN, plików wysyłanych drogą mailową, plików kopiowanych na dyski zewnętrzne, plików drukowanych. Konsola webowa musi umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe;

3.3. **Zarządzanie serwerem administracyjnym**

Serwer administracyjny musi:

3.3.1. Umożliwiać instalację na systemach Windows Server 2016 lub nowszych; Zamawiający dopuszcza pracę na systemach z rodziny GNU/Linux pod warunkiem, że oferowana dystrybucja posiada wsparcie producenta co najmniej do końca roku 2024 (dystrybucje LTS).

3.3.2. Współpracować z bazą danych MS SQL Server 2016 i nowszymi; Zamawiający dopuszcza wykorzystanie innych silników bazodanowych pod warunkiem, że posiadają one wsparcie producenta co najmniej do końca roku 2024.

3.3.3. Umożliwiać zarządzanie za pośrednictwem interfejsu graficznego (konsola);

3.3.4. Umożliwiać zarządzanie bazą danych poprzez określone zadania np.: wykonanie kopii bazy danych; usunięcie kopii bazy danych, usunięcie bazy danych, wprowadzenie ustawień dla kopii bazy danych. Zadania te powinny być dostępne z poziomu konsoli wraz z możliwością określenia automatycznego powtarzania zadań;

3.3.5. Posiadać funkcje automatycznej kopii bazy danych programu DLP w określonym przez administratora harmonogramie;

3.3.6. Posiadać możliwość zdefiniowania w programie przedziału czasowego dla kopii zapasowej bazy programu;

3.3.7. Komunikować się ze stacjami roboczymi wyłącznie za pomocą instalowanego na nich agenta;

3.3.8. Umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych;

3.3.9. Umożliwiać przygotowanie pliku instalacyjnego agenta za pośrednictwem konsoli zarządzającej.
Zamawiający dopuszcza sytuacje gdy producent oprogramowania będzie oferować pliki instalacyjne do dystrybucji poprzez SCCM;
3.3.10. Posiadać funkcjonalność aktualizacji własnych komponentów;
3.3.11. Mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych oraz aplikacji, z możliwością wyłączenia automatycznego pobierania;
3.3.12. Umożliwiać tworzenie nowych kont administratorów w konsoli programu, jak i ich usuwanie oraz klonowanie;
3.3.13. Posiadać możliwość automatycznej synchronizacji użytkowników oraz stacji roboczych z usługą Microsoft Active Directory;
3.3.14. Umożliwiać oznaczanie plików, które już znajdują się na stacjach roboczych i zasobach sieciowych;
3.3.15. Umożliwiać analizę lub oznaczanie nowo powstałych plików w oparciu o:

a) Aplikację, z której zostały utworzone.
b) Lokalizację lokalną oraz sieciową.
c) Adres URL, z którego został pobrany plik.
d) Format pliku,
e) Zawartość pliku,
f) Autora pliku opcjonalnie,
g) Datę utworzenia pliku opcjonalnie.

3.3.16. Serwer administracyjny musi mieć możliwość analizy lub oznaczania posiadanych plików wrażliwych w oparciu o:

a) Lokalizację lokalną oraz sieciową.
b) Format pliku.
h) Zawartość pliku,
i) Autora pliku opcjonalnie,
j) Datę utworzenia pliku opcjonalnie.

3.3.17. Oznaczanie plików, musi być dostępne dla wszystkich formatów plików oraz w oparciu o dowolną aplikacje;
3.3.18. Posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania;
3.3.19. Umożliwiać określenie stref urządzeń pamięci masowej, drukarek fizycznych, sieciowych, lokalizacji sieciowych, adresów mailowych oraz

domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu. Strefy muszą posiadać możliwość dodania elementów ręcznie oraz elementów, które były podłączane do stacji roboczych;

3.3.20. Posiadać funkcjonalność konsoli webowej, która umożliwia przeglądanie informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików wysyłanych do sieci, plików pobieranych z sieci, plików wysyłanych drogą mailową, plików kopiowanych na nośniki zewnętrzne;

3.4. **Zarządzanie konsolą webową**

Konsola webowa musi:

3.4.1. Umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe;

3.4.2. Umożliwiać dodanie klucza licencji;

3.4.3. Umożliwiać konfigurację/zmianę domyślnego serwera SMTP;

3.4.4. Umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością deaktywacji tego oprogramowania oraz pobrania pakietu najnowszej wersji;

3.4.5. Umożliwiać generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu;

3.4.6. Udostępniać konfigurowalny system paneli (ang. dashboard), operujący na różnych poziomach szczegółowości, z możliwością uwzględnienia różnych kanałów komunikacyjnych oraz możliwością wersjonowania (dostępu do danych historycznych panelu);

3.5. **Ochrona danych przesyłanych za pośrednictwem WWW**

Zamawiane oprogramowanie musi:

3.5.1. Umożliwiać monitorowanie i blokowanie treści naruszających zasady polityki w kanale WWW (http i https);

3.5.2. Umożliwiać, aby polityki chroniące informacje posiadały co najmniej możliwość konfiguracji:

a) Poprzez użycie centralnych polityk zdefiniowanych dla innych kanałów komunikacji;

b) W zależności od rodzaju użytkownika, także w oparciu o dane pochodzące ze zintegrowanego repozytorium użytkowników (np. jednostka organizacyjna, dział, grupa);

c) W zależności od docelowych adresów IP, na których odbywa się komunikacja;

d) W zależności od rodzaju przesyłanych plików i posiadanych przez pliki metadanych (np. tagów);

3.5.3. Umożliwiać przeglądanie aktywności użytkowników przeglądanych stron WWW i aplikacji internetowych;

3.6. **Agent stacji końcowych**

Zamawiane oprogramowanie musi:

3.6.1. Wspierać następujące systemy operacyjne:

a) Microsoft Windows 8.1 (wersja x64)

b) Microsoft Windows 10 (wersja x64)

c) Mac OS X 10.15.x i wyżej

3.6.2. Zapewniać ochronę i monitoring urządzenia końcowego bez względu na to, czy komputer jest podłączony do sieci czy nie;

3.6.3. Posiadać możliwość instalacji agenta na stacjach końcowych za pośrednictwem systemu SCCM;

3.6.4. Umożliwiać zabezpieczenie przed wyłączeniem/zawieszeniem lub dezinstalacją przez nieuprawnionego użytkownika.

3.6.5. Umożliwiać lokalne przechowywanie informacji w przypadku zerwania połączenia z serwerem zarządzającym, do czasu ponownego połączenia;

3.6.6. Umożliwiać wyświetlanie powiadomień (np. okno pop-up) dla użytkowników w języku polskim;

3.7. **Ochrona danych przesyłanych za pośrednictwem poczty e-mail**

Zamawiane oprogramowanie musi:

3.7.1. Umożliwiać identyfikację treści i załączników wiadomości mailowych m.in.: numery kart kredytowych, PESEL, określone ciągi znaków zdefiniowane przez administratora oraz umożliwiać powiadomienie o tym użytkownika;

3.7.2. Nadzorować wysyłane informacje kanałem poczty email (SMTP, POP3, IMAP oraz ich szyfrowane odpowiedniki)

3.7.3. Umożliwiać identyfikację oznaczonych plików w wiadomościach mailowych wysyłanych za pośrednictwem poczty mailowej;

3.7.4. Współpracować z klientem pocztowym MS Outlook;

3.7.5. Umożliwiać skanowanie plików poczty Microsoft zapisanych w formacie PST,

3.7.6. Umożliwiać dodawanie własnych nagłówków (X-HEADER) do wysyłanej poprzez klienta pocztowego wiadomości pocztowej.

3.8. **Monitorowanie bezpieczeństwa sieci Zamawiającego**

Zamawiane oprogramowanie musi:

3.8.1. Umożliwiać wykonywanie monitoringu sieciowego bez wywoływania dodatkowych opóźnień w transmisji danych, ani powodowania dodatkowych pojedynczych punktów awarii;

3.8.2. Analizować sieć co najmniej na poziomie rozróżniania protokołów sieciowych transmisji wraz z numerami portów TCP/IP, a ponadto ruch (z możliwością deszyfracji), odbywający się w kanale pocztowym email i kanale WWW, powinien być wykrywany za pomocą sygnatur (w tym monitorować załączniki poczty email oraz web-mail i inne usługi wykorzystujące np. protokół web - HTTP);

3.8.3. Umożliwiać monitorowanie ruchu przesyłanych plików np. poprzez FTP oraz p2p;

3.8.4. Umożliwiać monitoring usług na niestandardowych portach oraz zakresach portów.

3.8.5. Umożliwiać monitoring sklasyfikowanych i oznaczonych plików w sieci Zamawiającego oraz powiadamiać o próbach przesyłania tak oznaczonych plików dowolnym kanałem na zewnątrz firmy Zamawiającego;

3.9. **Wykrywanie wycieków danych**

Zamawiane oprogramowanie musi zapewniać:

3.9.1. Inspekcję zawartości plików i załączników,

3.9.2. Inspekcję plików skompresowanych (w tym spakowanych wielokrotnie),

3.9.3. Mechanizm wykrywania wycieku danych uwzględniający brak konieczności umieszczania wzorca danych na urządzeniu końcowym (stacji roboczej),

3.9.4. Możliwość konstrukcji polityk (tworzenia reguł wewnątrz polityk, ich edycji i przenoszenia pomiędzy politykami);

3.9.5. Możliwość wprowadzania szczególnych wyjątków w politykach, w których na podstawie dodatkowych kryteriów wykluczających dane podlegające zakazowi mogą być dystrybuowane;

3.9.6. Możliwość identyfikacji i wysyłania alarmów dla zdarzeń:

a) odmowy dostępu dla użytkownika do:

I. lokalizacji sieciowych,

II. stron internetowych,

III. aplikacji,

IV. pliku,

V. folderu;

b) zablokowanie możliwości przenoszenia oraz kopiowania danych;

c) podłączenie nieznanych urządzeń;

d) zablokowanie podłączonego urządzenia;

e) podłączenie nowej drukarki;

f)przekroczenie dopuszczalnego limitu drukowanej liczby stron;

g) zablokowanie drukowania;

h) kopiowanie oznaczonego pliku na nośnik zewnętrzny (np. pamięć USB);

3.9.7. Możliwość wykrywania zdefiniowanych informacji na podstawie zawartości plików (np. dokumentacja finansowa, kod źródłowy, oprogramowanie), z uwzględnieniem możliwości tworzenia wzorców takich dokumentów;

3.9.8. Możliwość ochrony wzorcowych dokumentów zawierających wrażliwe dane, bez konieczności używania słów kluczowych;

3.9.9. Możliwość wykrywania, przy użyciu ww. mechanizmu, nieustrukturyzowanych danych rozmieszczonych w wielu miejscach organizacji (dane w ruchu), a także nowych i nigdy niewidzianych plików, spoza organizacji;

3.9.10. Możliwość tworzenia reguł opartych co najmniej o: słowa kluczowe i zdania kluczowe,

3.9.11. Możliwość tworzenia reguł na podstawie wyrażeń regularnych, także zgodnych z REGEXP,

3.9.12. Możliwość wykorzystania predefiniowanych lub umożliwienie tworzenia wzorców opisowych dla poszukiwanych informacji;

3.9.13. Możliwość walidacji wykrytych informacji (np. wyliczanie sum kontrolnych dla numeru PESEL) oraz definiowania walidacji;

3.9.14. Możliwość edycji dostarczonych wzorców opisowych, walidatorów oraz możliwość tworzenia nowych, także na ich podstawie;

3.9.15. Możliwość analizy zewnętrznych, zabezpieczonych szyfrowaniem lub hasłem plików (w tym po zmianie rozszerzenia pliku), w celu ich weryfikacji i ewentualnego wykonania akcji (np. blokady) jeśli zostaną ujęte w polityce DLP;

3.9.16. Umożliwiać integrację z systemami klasy SIEM w zakresie przesyłania definiowalnej informacji o zdarzeniach lub incydentach dotyczących wycieku informacji; Zamawiający posiada i wykorzystuje oprogramowanie Splunk ES.

3.10. **Reakcja na wyciek danych**

Zamawiane oprogramowanie musi zapewniać:

3.10.1. Możliwość wysyłania powiadomienia w formie wiadomości mailowych, których treść musi być modyfikowalna przez administratora i obsługiwać co najmniej język polski i angielski (z uwzględnieniem mechanizmu tworzenia szablonów treści tych maili);

3.10.2. Możliwość automatycznego poinformowania o wykrytym naruszeniu polityk, co najmniej nadawcy, jak i innych określonych osób (np. administratora),

3.10.3. Możliwość wyświetlenia komunikatu dla użytkownika naruszającego politykę (na jego stacji roboczej) oraz umożliwienie temu użytkownikowi podjęcia określonych akcji (np. dalszej wysyłki informacji lub tylko wyświetlenia zdefiniowanego komunikatu i wygenerowaniu alertu widocznego dla administratora);

3.10.4. Możliwość podejmowania automatycznych oraz semi-automatycznych (wymagających udziału uprawnionej osoby) akcji naprawczych w przypadku wykrycia naruszenia polityki – reakcje te muszą być uzależnione od typu polityki, kategorii i wagi incydentu, liczby podobnych zdarzeń, kanału komunikacji (protokołu komunikacji);

3.10.5. Możliwość zdefiniowania akcji (np. blokowania) w przypadku naruszenia więcej niż jednej polityki.

3.10.6. Możliwość zabezpieczenia kopii plików, naruszających politykę bezpieczeństwa w momencie wykrycia naruszenia, w celu zabezpieczenia i

ochrony zgromadzonego materiału dowodowego incydentów;

3.11. **Obsługa zdarzeń wycieku danych**

Oprogramowanie musi zapewniać następujące funkcje:

3.11.1. Wizualizacja zdarzeń/incydentów musi być realizowana w sposób zrozumiały, przejrzysty i czytelny dla operatorów spoza działów IT i bezpieczeństwa informatycznego, a każdy element zdarzenia powinien być jasno opisany, ze szczególnym uwidocznieniem: kanału transmisji, powodu wygenerowania oraz elementów naruszających politykę;

3.11.2. Opis incydentu powinien zawierać informacje podstawowe, co najmniej: imię i nazwisko, datę i czas wystąpienia incydentu, podjętą czynność, rodzaj incydentu;

3.11.3. Grupy incydentów muszą być możliwe do wyeksportowania z poziomu konsoli operatora, w formie czytelnej i przejrzystej dla użytkowników spoza IT oraz zapisane w formacie pliku łatwym do obsługi dla tych użytkowników (np. PDF, HTML lub CSV)

3.11.4. Mechanizm manualnego wywoływania akcji dotyczącej danego zdarzenia/incydentu (np. zablokowania oznaczonych plików przed wysyłaniem);

3.11.5. Blokowanie oraz zezwalanie na zapisywanie, przenoszenie do innej lokalizacji w tym na dyski zaszyfrowane, zewnętrzne i sieciowe plików ujętych w polityce (również pliki oznaczonych);

3.11.6. Możliwość utworzenia białej oraz czarnej listy urządzeń przeznaczonych do zapisu (np. dyski, pamięci USB) i drukarek;

3.11.7. Blokowanie oraz zezwalanie na wysyłanie plików (w tym oznaczonych) za pośrednictwem klienta pocztowego, folderów synchronizacji z usługami chmury (np. Google Drive, One Drive, SharePoint);

3.11.8. Możliwość utworzenia białej oraz czarnej listy domen pocztowych i adresów mailowych;

3.11.9. Blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików (w tym oznaczonych) poprzez usługę pulpitu zdalnego;

3.11.10. Blokowanie oraz zezwalanie na wykonywanie zrzutów ekranów, kopiowania treści plików do schowka, nagrywania na płyty CD/DVD, SD/CF oraz drukowania wirtualnego plików;

3.11.11. Globalne zablokowanie oraz zezwolenie na korzystanie z określonych folderów lokalnych, dysków sieciowych, dysków o określonej literze oraz folderów synchronizacji z usługami chmury;

3.12. **Raportowanie i analityka**

Zamawiane oprogramowanie musi zapewniać:

3.12.1. Możliwość filtrowania przy użyciu różnych warunków, w tym zmiennych, atrybutów oraz możliwość ich wykorzystywania dla różnych filtrów;

3.12.2. Możliwość łatwego przechodzenia z raportu ogólnego do szczegółowych danych,

3.12.3. Możliwość wygenerowania raportu podsumowującego incydenty i trendy w rozbiciu na różne atrybuty, (także pobierane z repozytorium użytkowników), z możliwością ograniczenia zakresów czasowych;

3.12.4. Możliwość uproszczonego i zaawansowanego wyszukiwania incydentów z określonych grupy, w tym także przy użyciu określonych atrybutów;

3.12.5. Możliwość uzyskania raportów w czytelnych formatach, takich jak PDF oraz formatach do dalszego użytku,np. CSV lub XLS;

3.12.6. Możliwość raportowania: reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, podsumowania korzystania z urządzeń oraz ich typów;

3.12.7. Możliwość, generowania raportów w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu;

3.12.8. Automatyczne generowanie raportów, wysyłanych za pośrednictwem poczty mailowej;

3.12.9. Generowanie raportu z wykorzystaniem różnych opcji językowych (np. polski, angielski);

3.13. **Szczegółowe funkcjonalności w zakresie klasyfikacji dokumentów**

Zamawiane oprogramowanie musi:

3.13.1. Umożliwiać oznaczanie dokumentów w formie tagów lub metadanych, rozpoznawanych przez systemy informatyczne;

3.13.2. Umożliwiać definiowane własnych kategorii oraz polityk klasyfikacji wraz z możliwością tworzenia różnych klas i polityk klasyfikacji z możliwością ich przypisania do grup użytkowników,

jednostkowych użytkowników i ról w systemie, także wynikających z repozytorium użytkowników (np. Active Directory);

3.13.3. Umożliwiać ustalanie zasad automatycznych zmian w klasyfikacji dokumentów;

3.13.4. Posiadać mechanizm automatycznego rozwiązywania konfliktów klasyfikacji i wykonywania definiowalnych akcji;

3.13.5. Zapewniać interaktywność mechanizmu klasyfikacji z użytkownikiem (np. notyfikacja lub żądanie świadomego potwierdzenia wykonania określonej czynności);

3.13.6. Posiadać scentralizowaną bazę logów, w tym logów audytowych, zawierających dane dotyczące czynności administratorów i operatorów oprogramowania, a także użytkowników, obejmujące dane o klasyfikacji informacji oraz o ewentualnych niezgodnościach;

3.13.7. Umożliwiać definiowanie własnego nazewnictwa dla poszczególnych kategorii dokumentów (np. dane poufne, dane tajne);

3.13.8. Umożliwiać integrację z oprogramowaniem MS Office oraz Office 365, które posłuży między innymi do wybrania kategorii dokumentu, w szczególności integrować się z oknem tworzenia/odczytu oraz oknem "Zapisz/Zapisz jako";

3.13.9. Zapewniać możliwości klasyfikacji plików z menu kontekstowego dla plików i katalogów (Domyślnie w systemie Windows: kliknięcie prawym przyciskiem myszki skutkuje wywołaniem menu kontekstowego);

3.13.10. Zapewnić wymuszenie klasyfikacji dokumentu przed jego wydrukowaniem lub inną formą udostępnienia;

3.13.11. Umożliwiać klasyfikację plików PDF (skany), archiwów, plików tekstowych, obrazów oraz dodawanie do dokumentów metadanych w postaci np. tagu;

3.13.12. Zapewniać automatyczną klasyfikację informacji bazującą na zawartości danych zgodnie z polityką firmy (np. poprzez użyte słowa kluczowe, wyrażenia regularne, format).

3.13.13. Zapewniać automatyczną klasyfikację informacji w oparciu o kontekst informacji (np. wybrany właściciel informacji lub autor, określony odbiorca lub grupa użytkowników);

3.14. **Szczegółowe funkcjonalności w zakresie usługi szyfrowania plików i danych**

Zamawiane oprogramowanie musi:

3.14.1. Realizować szyfrowanie całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM;

3.14.2. Realizować szyfrowanie dysków zewnętrznych w oparciu o funkcjonalność BitLocker, szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika;

3.14.3. Umożliwiać szyfrowanie dokumentów w oparciu o polityki związane z klasyfikacją użytkownika lub automatyczną analizą treści, realizowane w sposób automatyczny,

3.14.4. Zapewniać możliwość przechowywania kluczy szyfrujących w infrastrukturze zamawiającego;

3.14.5. Posiadać możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła;

3.14.6. Zapewnić, aby szyfrowanie dokumentów działało poprawnie w systemach MS Windows 8.1, 10 oraz Mac OS X 10.15;

4. Zakres wsparcia technicznego i serwisu dla zakupionego oprogramowania:

4.1. Zakres wsparcia, w terminie obowiązywania umowy, obejmuje:

4.1.1. Dostęp do pomocy technicznej w dni robocze w godzinach 8.00-16.00, przez okres trwania umowy;

4.1.2. Usługę konsultacji w zakresie konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości max 80 roboczogodzin dla systemu klasy DLP (ang. man-day), zgodnie z zapotrzebowaniem Zamawiającego, możliwych do wykorzystania w terminie obowiązywania umowy. Zamawiający zastrzega sobie możliwość korzystania z usługi wsparcia technicznego i serwisu w miarę identyfikowanych potrzeb, przez co możliwe jest nie wykorzystanie pełnej puli roboczogodzin. Minimalna liczba roboczogodzin jaką wykorzysta Zamawiający i za jaką zobowiązuje się wypłacić Wykonawcy wynagrodzenie wynosi 30, przez cały okres obowiązywania umowy.

4.1.3. Dostęp do poprawek i nowych wersji oprogramowania i/lub systemu;

4.1.4. Dostęp do dokumentacji technicznej;

4.1.5. Dostęp do konta wsparcia oprogramowania, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.

Załącznik Nr 2 do SWZ

FORMULARZ OFERTY

dla Narodowego Centrum Badań i Rozwoju

Ja/my* niżej podpisani:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

działając w imieniu i na rzecz:

.....

.....

(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)

Adres:

……

Kraj ……..

REGON ……

NIP: ……..

TEL. …….

Adres skrzynki ePUAP ……

adres e-mail:……

(na który Zamawiający ma przesyłać korespondencję)

Wykonawca jest mikro, małym, średnim przedsiębiorcą - **TAK/NIE***

Ubiegając się o udzielenie zamówienia publicznego na ***dostawę systemu ochrony przed wyciekiem informacji DLP (Nr postępowania 16/21/TPBN)***

1. **SKŁADAMY OFERTĘ** na realizację przedmiotu zamówienia w zakresie określonym w Specyfikacji Warunków Zamówienia, na następujących warunkach:

1.1. **Cena oferty netto** za realizację całego zamówienia wynosi: ……..……. zł, (słownie:……),

1.2. **Cena oferty brutto** za realizację całego zamówienia wynosi: ……..……. zł, (słownie:……).

w tym podatek od towarów i usług (VAT), wg stawki: ……. %

w tym:

zamówienie podstawowe:

Cena oferty netto za realizację zamówienia w zakresie zamówienia podstawowego wynosi: ……..……. zł, (słownie:……),

Cena oferty brutto za realizację zamówienia w zakresie zamówienia podstawowego wynosi: ……..……. zł, (słownie:……).

w tym podatek od towarów i usług (VAT), wg stawki: ……. %

zamówienie opcjonalne:

Cena oferty netto za realizację zamówienia w zakresie zamówienia opcjonalnego wynosi: ……..……. zł, (słownie:……),

Cena oferty brutto za realizację zamówienia w zakresie zamówienia opcjonalnego wynosi: ……..……. zł, (słownie:……).

w tym podatek od towarów i usług (VAT), wg stawki: ……. %

z uwzględnieniem cen jednostkowych wskazanych w tabeli poniżej:

l.p.	Nazwa	Nazwa oferowanego systemu	Ilość	Cena jednostkowa netto	Wartość netto (cena jednostkowa*ilość)	Stawka VAT	Wartość brutto
Zamówienie podstawowe							
1.	System klasy DLP – 800 stanowisk		800				
2.	Wsparcie techniczne i serwis		80 godzin				
Zamówienie opcjonalne							
1	System klasy DLP – 160 stanowisk		160				
				suma			

2. **OFERUJEMY,** dostarczenie licencji w terminie …[3] dni roboczych od dnia zawarcia umowy.
3. **OŚWIADCZAMY,** że zamówienie wykonamy w terminie podanym przez Zamawiającego.

[3] W przypadku niewypełnienia pozycji Zamawiający uzna, iż Wykonawca zaoferował 10 dniowy termin dostarczenia licencji.

4. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i akceptujemy oraz spełniamy wszystkie warunki w niej zawarte.
5. **OŚWIADCZAMY**, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.
6. **OŚWIADCZAMY**, że jesteśmy związani niniejszą ofertą od dnia upływu terminu składania ofert do dnia 08.05.2021 roku.
7. **OŚWIADCZAMY**, że zapoznaliśmy się z Projektowanymi Postanowieniami Umowy, określonymi w Załączniku nr 4 do Specyfikacji Warunków Zamówienia i ZOBOWIĄZUJEMY SIĘ, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.
8. **AKCEPTUJEMY** Projektowane Postanowienia Umowne, w tym warunki płatności oraz termin realizacji przedmiotu zamówienia podany przez Zamawiającego.
9. **OŚWIADCZAM**, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[4] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**
10. Wraz z ofertą **SKŁADAMY** następujące oświadczenia i dokumenty:

1. ……
2. ……
3. ……

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

Informacja dla Wykonawcy:

Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.

** niepotrzebne skreślić*

*** w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO Wykonawca nie składa oświadczenia (usunięcie treści oświadczenia następuje np. przez jego wykreślenie).*

[4] rozporządzenie 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

Załącznik nr 3 do SWZ

Nazwa Wykonawcy, w imieniu którego składane jest oświadczenie:

.....

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

WSTĘPNE OŚWIADCZENIE WYKONAWCY[1]

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako: Pzp)

DOTYCZĄCE PODSTAW WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. *dostawę systemu ochrony przed wyciekiem informacji DLP (Nr postępowania 16/21/TPBN)* prowadzonego przez Narodowe Centrum Badań i Rozwoju (NCBR), z siedzibą w Warszawie (00-695), przy ul. Nowogrodzkiej 47a (NIP: 701-007-37-77, REGON: 141032404), oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 art. 109 ust. 1 pkt 4, 5, 7 ustawy Pzp.

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub 6 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:

……

……

……

[1] *Pouczenie o odpowiedzialności karnej Art. 297 § 1 Kodeksu karnego* (Dz. U. Nr 88 poz. 553 z późn. zm.)*:*
„Kto w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi – kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, elektronicznego instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.”

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

Załącznik nr 4 do SWZ

PROJEKTOWANE POSTANOWIENIA UMOWY

/osobny plik/

Załącznik nr 6 do SWZ

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Lp.	Pytanie	Odpowiedź	Uwagi
1	Czy podmiot przetwarzający dane osobowe planuje wyznaczyć/wyznaczył Inspektora Ochrony Danych Osobowych (IOD)?	* - tak zaplanowano wyznaczenie - tak wyznaczono - nie zaplanowano wyznaczenia (uzasadnienie: np. nie jest wymagane przepisami prawa) - zaplanowano wyznaczenie (kiedy: podać przewidywaną datę)	
2	Jeżeli nie został wyznaczony IOD to proszę o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu….., stanowisko/funkcja…., numer tel.	
3	Czy podmiot przetwarzający dane osobowe wprowadził środki techniczne i organizacyjne, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych?	* TAK/NIE/INNE	
4	Czy podmiot przetwarzający dane osobowe korzysta z dalszych przetwarzających dane osobowe w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	* TAK/NIE	
5	Czy dane osobowe będą przekazywane poza Europejski Obszar Gospodarczy?	* TAK/NIE	

*Właściwe podkreślić/uzupełnić

Oświadczenie:

W imieniu podmiotu przetwarzającego dane osobowe /nazwa podmiotu/, oświadczam, że powyżej przekazane informacje są zgodne z prawdą. W przypadku zmiany któregokolwiek z ww. elementów, zobowiązuje się niezwłocznie (nie później niż w terminie 7 dni od wystąpienia zdarzenia) powiadomić o tym Narodowe Centrum Badań i Rozwoju.

…….. ……

data *Imię i nazwisko*

podpisano elektronicznie

Ocena Inspektora Ochrony Danych w Narodowym Centrum Badań i Rozwoju

Wypełnia IOD NCBR:

Rekomenduję/nie rekomenduję zawarcie umowy powierzenia przetwarzania danych osobowych.

Uzasadnienie:

……

……

……

…….. ……

data podpis

Załącznik Nr 7 do SWZ

Klauzula informacyjna dotycząca przetwarzania danych osobowych

1. Zgodnie z art. 13 ust. 1 i 2 oraz 14 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:
   - administratorem Pani/Pana danych osobowych jest Narodowe Centrum Badań i Rozwoju, ul. Nowogrodzka 47a, 00-695 Warszawa (dalej NCBR)*;*
   - w sprawach związanych z Pani/Pana danymi proszę kontaktować się z Inspektorem Ochrony Danych, kontakt pisemny za pomocą poczty tradycyjnej na adres ……, bądź pocztą elektroniczną na adres e-mail: iod@ncbr.gov.pl**;**
   - Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia zamówienia publicznego na *dostawę systemu ochrony przed wyciekiem informacji DLP (Nr postępowania 16/21/TPBN)*, udzielonego w trybie podstawowym bez negocjacji art. 275 pkt 1 ustawy Pzp;
   - Pani/Pana dane osobowe zostały pozyskane od podmiotu, który odpowiedział na ogłoszenie o postępowaniu o udzielenie zamówienia publicznego wskazanym powyżej;
   - NCBR będzie przetwarzał Pani/Pana dane w zakresie danych kontaktowych, informacji o zatrudnieniu, stopni naukowych oraz inne w zakresie podanym przez podmiot składający ofertę w odpowiedzi na ogłoszenie o udzieleniu zamówienia publicznego;
   - odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy Pzp;
   - Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 i 4 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy, a następnie w celu archiwalnym przez okres zgodny z instrukcją kancelaryjną NCBR i Jednolitym Rzeczowym Wykazem Akt;
   - obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
   - w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
   - posiada Pani/Pan:

   − na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

   − na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych, przy czym skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

− na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO oraz art. 19 ust. 3 ustawy Pzp ;

− prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

- nie przysługuje Pani/Panu:

− w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

− prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

− na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

2. Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

Załącznik nr 8 do SWZ

Oświadczenie, o którym mowa w art. 117 ust. 4 ustawy z dnia 11 września 2019 r.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia

Działając na podstawie art. 117 ust. 4 ustawy Pzp oświadczam, iż Wykonawcy wspólnie ubiegający się o udzielenie zamówienia zrealizują przedmiotowe zamówienie w zakresie określonym w tabeli:

l.p.	Nazwa Wykonawcy	Zakres zamówienia realizowany przez Wykonawcę
1.		
2.		

……., dnia ……. r.

……

Imię i nazwisko

podpisano elektronicznie

Załącznik nr 9 do SWZ

WYKAZ DOSTAW

Dotyczy: zamówienia publicznego, którego przedmiotem jest ***dostawę systemu ochrony przed wyciekiem informacji DLP (Nr postępowania 16/21/TPBN).***

W zakresie niezbędnym do wykazania spełnienia warunku wiedzy i doświadczenia, o którym mowa w rozdziale VII pkt 2.1 SWZ, w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie.

	Wymaganie Zamawiającego: **w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonał należycie, a w przypadku świadczeń okresowych lub ciągłych wykonuje należycie co najmniej dwie dostawy systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention), dla co najmniej 400 stanowisk każda i o wartości zamówienia co najmniej 100 000 zł brutto każda.**	
Lp.	Wykonana usługa ……	
1.	**Nazwa i zakres dostawy**	…….. ……..
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej dostawy)*	od ……/……/……..... do ……/……/……..... *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał wykonanie dostawy)	…… …… *(nazwa i adres)*
	Wartość brutto	……
	Dokument potwierdzający należyte wykonanie wyżej wymienionej dostawy	Nr strony oferty - ……..……
2.	**Nazwa i zakres dostawy**	……..

		……..
	Data wykonania *(należy podać datę rozpoczęcia i zakończenia wskazanej dostawy)*	od ……/……/…… do ……/……/…… *(dzień / miesiąc / rok)*
	Odbiorca (podmiot, który zlecał wykonanie dostawy)	…… …… *(nazwa i adres)*
	Wartość brutto	……
	Dokument potwierdzający należyte wykonanie wyżej wymienionej dostawy	Nr strony oferty - ……

Do powyższego wykazu załączam dowody potwierdzające, że wskazane w nim usługi, o których mowa w rozdziale VII pkt 2.1 SWZ, zostały wykonane należycie. [2]

……, dnia …… r.

……

Imię i nazwisko

podpisano elektronicznie

[2] W przypadku większej liczby usług należy powielić tabelę