- W Z Ó R -

**UMOWA Nr SPKSO/ZP- ……../2022**
**NA DOSTAWĘ LICENCJI I OPROGRAMOWANIA WRAZ Z WDROŻENIEM**
**( P A K I E T N R 1 )**

zawarta w dniu **……** w Warszawie pomiędzy:

**Samodzielnym Publicznym Klinicznym Szpitalem Okulistycznym w Warszawie,** działającym na stałe pod adresem: ul. Sierakowskiego 13, 03-709 Warszawa, a tymczasowo pod adresem: ul. Marszałkowska 24/26, 00-576 Warszawa, na podstawie wpisu do Krajowego Rejestru Sądowego pod numerem KRS: 0000113950, NIP: 113-21-68-300, REGON: 016084355, zwanym dalej **„Zamawiającym”**, reprezentowanym przez:

Prof. dr hab. n. med. Jacka P. Szaflika – Dyrektora
a
**spółką ……** z siedzibą w ……, adres: ……, wpisaną do rejestru przedsiębiorców prowadzonego przez ……, pod nr KRS: ……, NIP: ……, REGON: ……, o kapitale zakładowym w wysokości ……[1], zwaną dalej „**Wykonawcą**”, reprezentowaną przez:
……, w imieniu którego(-ej) działa ……, na podstawie upoważnienia nr …… z dnia ……, które nie wygasło i nie zostało odwołane**;**.

zwanych dalej łącznie: Stronami

Zważywszy, że:

(A) Zamawiający zawarł w dniu 16 września 2022 r. umowę Nr 59/2022 z Narodowym Funduszem Zdrowia - Mazowieckim Oddziałem Wojewódzkim o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwaną dalej : Umowa z NFZ ;

(B) Zamawiający przeprowadził postępowanie o udzielenie zamówienia publicznego o numerze sprawy ZP/10/2022 przeprowadzonego w trybie podstawowym bez negocjacji, o którym mowa w art. 275 pkt 1 Ustawy PZP, zwane dalej „Postępowaniem”, którego przedmiotem jest : Dostawa oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowana w wykonaniu umowy o finansowanie ze środków pochodzących z funduszu przeciwdziałania COVID-19 w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, obejmujące 3 pakiety :

1) Pakiet Nr 1 , którego przedmiotem jest dostawa licencji z oprogramowaniem i wdrożeniem, obejmująca :

[1] Dotyczy spółki kapitałowej. Jeżeli Wykonawcą nie będzie spółka kapitałowa należy podać informacje odpowiednie do formy prawnej działalności gospodarczej prowadzonej przez Wykonawcę.

a) udzielenie licencji na oprogramowanie oraz wdrożenie centralnego systemu ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania – XDR;

b) dostawę i wdrożenie oprogramowania kontroli dostępu i zarządzania tożsamościami użytkowników oraz dostępu komputerów do sieci lokalnej;

2) Pakiet Nr 2 , którego przedmiotem jest :

„ Szkolenie dot. cyberbezpieczeństwa wykonane na potrzeby i na podstawie Zarządzenia Nr 117/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 wrzesnia 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów informatycznych świadczeniodawców" ;

3) Pakiet Nr 3 , którego przedmiotem jest :

„Audyt poziomu bezpieczeństwa teleinformatycznego";

(C) Wykonawca oświadcza, że zgodnie ze stanem faktycznym i prawnym aktualnym w chwili zawarcia niniejszej umowy nie zachodzą w stosunku do niego podstawy wykluczenia, o których mowa w art. 108 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.), zwanej dalej: Ustawą PZP oraz w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2022 r. poz. 835, z późn. zm.);

(D) oferta złożona przez Wykonawcę została wybrana jako najkorzystniejsza w Postępowaniu **w zakresie Pakietu Nr 1 ;**

została zawarta pomiędzy Stronami umowa o następującej treści:

## § 1.
## DEFINICJE

1. Następujące wyrażenia i określenia użyte w niniejszej Umowie, w różnych przypadkach i liczbie, będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisanymi dużą literą w celu podkreślenia, że są to pojęcia zdefiniowane:
   1) **Strony** – Zamawiający i Wykonawca wymienieni w komparycji **Umowy**;
   2) **Umowa** – niniejsza umowa w sprawie zamówienia publicznego wraz z wymienionymi w jej treści dokumentami nazwanymi i nienazwanymi załącznikami, regulująca wynikające z niej i związane z jej wykonaniem, prawa i obowiązki Stron;
   3) **OPZ –** Opis Przedmiotu Zamówienia, w którym wyszczególnione zostały wszystkie wymagania jakościowe i techniczne odnoszące się do przedmiotu zamówienia, stanowiący Załącznik nr 2 do Umowy ;
   4) **Oprogramowanie –** aplikacje komputerowe określone w OPZ ;
   5) **Licencja** - umowa na korzystanie z Oprogramowania, zawierana za pośrednictwem Wykonawcy, pomiędzy podmiotem, któremu przysługują majątkowe prawa autorskie do Oprogramowania, a Zamawiającym, zawierająca kod alfanumeryczny dający Zamawiającemu prawo do bezterminowego korzystania, uruchamiania i użytkowania Oprogramowania na zasadach określonych w Załączniku nr 2 do Umowy oraz na ogólnych warunkach producenta Oprogramowania;
   6) **Przedmiot Umowy – (Pakiet Nr 1)** dostawa licencji z oprogramowaniem i

wdrożeniem, obejmująca :

a) udzielenie licencji na oprogramowanie oraz wdrożenie centralnego systemu ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania – XDR;

b) dostawę i wdrożenie oprogramowania kontroli dostępu i zarządzania tożsamościami użytkowników oraz dostępu komputerów do sieci lokalnej;

spełniających wymagania wyszczególnione w OPZ, który jest integralną częścią umowy i stanowi Załącznik nr 2 do Umowy.

7) **Produkty –** licencja i oprogramowanie wraz z wdrożeniem;

8) **Formularz asortymentowo-cenowy –** wykaz licencji i oprogramowania objętego przedmiotem Umowy, stanowiący Załącznik Nr 1 do Umowy;

9) **Cena –** wartość brutto przedmiotu Umowy, określona w Ofercie, wyrażona w postaci cen jednostkowych brutto za poszczególne pozycje wyspecyfikowanych Produktów;

10) **Miejsce lokalizacji –** miejsce wskazane przez Zamawiającego, do którego Wykonawca jest zobowiązany dostarczać Produkty zgodnie z niniejszą Umową, tj. siedziba tymczasowa ul. Marszałkowska 24/26, 00-576 Warszawa a z chwilą przeniesienia Szpitala do siedziby docelowej – ul. Józefa Sierakowskiego 13, 03-709 Warszawa;

11) **Aktualizacja Oprogramowania** – każda poprawka programistyczna Oprogramowania wykonana przez jego producenta, do której otrzymania i z której korzystania Zamawiający uprawniony jest na zasadach określonych w ogólnych warunkach producenta Oprogramowania;

12) **Dokumentacja Oprogramowania** – podręcznik użytkownika, instrukcje instalacji i obsługi Oprogramowania oraz instrukcje określające funkcje Oprogramowania;

13) **Przedstawiciele Stron** lub **Przedstawiciele Zamawiającego i Wykonawcy** – osoby wskazane w § 4 ust. 1 i 2, upoważnione na mocy postanowień Umowy do reprezentowania odpowiednio Zamawiającego lub Wykonawcy, w sprawach związanych z realizacją przedmiotu Umowy;

14) **Kodeks cywilny** – ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2022 r. poz. 1360);

2. Ilekroć w Umowie termin podawany jest w dniach, bez użycia określenia **„Dni robocze",** Strony rozumieją przez to dni kalendarzowe. W przypadku określenia terminu w Dniach roboczych, Strony rozumieją przez to dni od poniedziałku do piątku w godzinach od 8.00 do 14.00 z wyłączeniem dni ustawowo wolnych od pracy.
3. Ilekroć w Umowie występuje odniesienie do:
   1) **„formy pisemnej**", należy przez top rozumieć zastrzeżenie formy pisemnej lub formy elektronicznej , pod rygorem nieważności chyba, że w Umowie wprost przewidziano inny reżim niezachowania formy pisemnej niż nieważność (bezskuteczność);
   2) **„pisemności",** należy przez to rozumieć sposób wyrażenia informacji przy użyciu wyrazów, cyfr lub innych znaków pisarskich, które można odczytać i powielić, w tym przekazywanych przy użyciu środków komunikacji elektronicznej.

**§ 2.**

## PRZEDMIOT UMOWY I ZASADY REALIZACJI

1. Na podstawie niniejszej Umowy Wykonawca zobowiązuje się dostarczyć do Miejsca Lokalizacji Produkty, a Zamawiający zobowiązuje się odebrać i zapłacić Wykonawcy należną cenę za wykonanie Przedmiotu Umowy.
2. Realizacja Przedmiotu Umowy obejmuje w szczególności :
   1) centralny system ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania - XDR ……;
   2) system zarządzania dostępem użytkowników i urządzeń do sieci…….;
   3) prace wdrożeniowe w zakresie instalacji i konfiguracji systemów (w tym prace konfiguracyjne systemu uwierzytelniania opartego o protokół PEAP z protokołem EAP-TLS w wersji 802.1x oraz konfiguracja Captive Portal z autentyfikacją opartą na Self-registration);
   4) instruktaż powdrożeniowy dla 3 pracowników Zamawiającego obejmujący zakresem obsługę wdrożonych systemów.
3. Wykonawca zapewni wsparcie serwisowe przez okres wskazany w OPZ, obejmujące dostępność aktualizacji oprogramowania oraz rozwiązywanie problemów związanych z użytkowaniem dostarczonych systemów. Wsparcie serwisowe będzie realizowane w dni robocze od poniedziałku do piątku w godzinach 9:00-17:00.
4. Wykonawca oświadcza, że :
   1) posiada niezbędne kwalifikacje do pełnej realizacji Przedmiotu Umowy;
   2) jest uprawniony do wprowadzania urządzeń i oprogramowania do obrotu oraz udzielania licencji zgodnie postanowieniami ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 2021 r. poz. 1062 t.j., z późn. zm.) oraz, że dostarczy oprogramowanie wolne od wad.

5. Prawo do korzystania z Licencji na Oprogramowanie przechodzi na Zamawiającego z chwilą podpisania Protokołu Odbioru, o którym mowa w § 3 ust.1 Umowy, bez żadnych uwag.

6. Wykonawca zobowiązany jest dostarczyć najpóźniej do chwili podpisania Protokołu Odbioru, o którym mowa w § 3 ust.1 Umowy:

   1) Licencje na Oprogramowanie w postaci elektronicznej;
   2) dane dostępowe umożliwiające pobranie przez Zamawiającego Oprogramowania oraz Dokumentacji Oprogramowania w postaci elektronicznej.

7. Wykonawca jest w pełni odpowiedzialny za wszelkie wady prawne oprogramowania, w szczególności, jeżeli stanowią one własność osoby trzeciej lub są obciążone prawem osób trzecich, w tym również za ewentualne roszczenia osób trzecich, wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, wprowadzone do obrotu na terytorium RP.

8. Wykonawca przeprowadzi szkolenie dla pracowników IT Zamawiającego zgodnie z OPZ, w zakresie użytkowania wdrożonego systemu, w uzgodnionym między Stronami terminie.

9. W związku z realizacją Umowy Zamawiający jako administrator Danych osobowych swoich pracowników i pacjentów powierza Wykonawcy w trybie art. 28 rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem" lub ,,RODO") ich dane osobowe do przetwarzania , w zakresie i na zasadach oraz w celu określonym w umowie powierzenia przetwarzania danych osobowych, stanowiącej załącznik Nr 6 do Umowy.

## § 3.
## TERMIN I WARUNKI REALIZACJI PRZEDMIOTU UMOWY

1. Wykonawca zobowiązuje się zrealizować Przedmiot Umowy w zakresie opisanym w § 2 ust. 2 Umowy przy zachowaniu wymagań jakościowych i technicznych opisanych w OPZ, w nieprzekraczalnym terminie do dnia 30 listopada 2022 r. Wykonanie Przedmiotu Umowy przez Wykonawcę zostanie potwierdzone 'Protokołem odbioru' sporządzonym wg wzoru stanowiącego Załącznik nr 3 do Umowy.

2. Wykonawca dostarczy do miejsca Lokalizacji , zgodnie z warunkami określonymi w Umowie, Oprogramowanie oraz Dokumentację Oprogramowania oraz przekaże na adresy poczty elektronicznej wskazane w § 4 ust. 1 dane dostępowe umożliwiające pobranie przez Zamawiającego Oprogramowania oraz Dokumentacji Oprogramowania w postaci elektronicznej.

3. Wykonawca, z co najmniej 5-dniowym wyprzedzeniem, powiadomi drogą elektroniczną przedstawicieli Zamawiającego wskazanych w § 4 ust.1, o dacie dostawy Oprogramowania podając co najmniej:

1) numer niniejszej Umowy;

2) planowaną datę dostarczenia Przedmiotu Umowy.

4. Zamawiający zobowiązany jest niezwłocznie potwierdzić termin dostawy Przedmiotu Umowy. Zamawiający może określić inną datę dostawy Przedmiotu Umowy, nie późniejszą jednak niż w ciągu 2-ch dni od daty wskazanej przez Wykonawcę.

5. Odbiór Oprogramowania od Wykonawcy nastąpi w Miejscu Lokalizacji, w terminie 4 dni licząc od dnia jego dostarczenia i zostanie potwierdzony w formie Protokołu Odbioru podpisanego przez Przedstawicieli Zamawiającego i Wykonawcy, sporządzonego według wzoru stanowiącego Załącznik nr 3 do Umowy, z zastrzeżeniem ust 6.

6. Jeżeli przy dostawie lub odbiorze Oprogramowania Strony stwierdzą usterki bądź braki, Wykonawca zobowiązany jest do ich usunięcia w terminie uzgodnionym protokolarnie przez Strony. W takim przypadku potwierdzeniem odbioru Oprogramowania jest Protokół Odbioru sporządzony według wzoru stanowiącego Załącznik nr 3 do Umowy na dzień uzupełnienia braków lub usunięcia usterek. Postanowienia ust 5 stosuje się odpowiednio.

7. Termin przewidziany na dokonanie odbioru Oprogramowania przez Zamawiającego nie wlicza się do terminu wykonana Przedmiotu Umowy określonego w ust. 1, natomiast termin przewidziany na uzupełnienie braków lub usunięcie usterek przez Wykonawcę wlicza się do czasu przewidzianego na wykonanie Przedmiotu Umowy określonego w ust.1.

8.Zamawiający dopuszcza możliwość realizacji Przedmiotu Umowy w częściach, z zastrzeżeniem, że przedmiot Umowy zostanie dostarczony w całości w terminie

określonym w ust. 1. Dostawy częściowe mogą dotyczyć wyłącznie Oprogramowania opisanego w Załączniku nr 1 do Umowy, tj. pozycji o zdefiniowanej cenie jednostkowej. Do odbioru części Przedmiotu Umowy, postanowienia ust. 2-7 stosuje się odpowiednio.

## § 4.
## PRZEDSTAWICIELE STRON

1. Do reprezentowania Zamawiającego w sprawach związanych z realizacją przedmiotu zamówienia oraz zgłaszania uwag dotyczących sposobu realizowania Umowy, upoważniony jest :
   – …… - Kierownik Działu IT, tel.: …, e-mail: ……
2. Do reprezentowania Wykonawcy w sprawach związanych z realizacją przedmiotu zamówienia oraz zgłaszania uwag dotyczących sposobu realizowania Umowy, upoważniony(-na) jest: …… - …… tel.: ……, e-mail: ……..
3. Zmiana osób, o których mowa w ust. 1 i 2, nie stanowi zmiany niniejszej Umowy, przez co nie wymaga dla swojej ważności zachowania formy pisemnej aneksu do Umowy i dokonywana będzie na podstawie oświadczenia osoby upoważnionej do reprezentowania Strony, przekazanego drugiej Stronie za pośrednictwem poczty elektronicznej.
4. Osoby wskazane w ust. 1 i 2 upoważnione są do dokonywania w imieniu odpowiednio Zamawiającego lub Wykonawcy czynności określonych w Umowie, z wyłączeniem zmiany postanowień Umowy, odstąpienia od Umowy lub jej rozwiązania.
5. Wszelkie informacje związane z realizacją Przedmiotu Umowy będą przekazywane za pośrednictwem poczty elektronicznej na dane kontaktowe wskazane w ust. 1 i 2, z wyjątkiem dokumentów, dla których w Umowie zastrzeżono formę pisemną.
6. Wykonawca przedkłada Zamawiającemu przy zawieraniu Umowy „Oświadczenie o zachowaniu poufności" stanowiące Załącznik Nr 4 do Umowy, podpisane przez osob/ę/y/ reprezentujące Wykonawcę oraz osob/ę/y wymienion/ą/e w ust. 2 oraz oświadcza, że zapoznał te osoby z treścią „Informacji o przetwarzaniu danych osobowych" stanowiącą Załącznik nr 5 do Umowy.

## § 5.
## WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za wykonany i odebrany Przedmiot Umowy wynagrodzenie w kwocie wynoszącej netto …… PLN (słownie: ……), zgodnie z cenami jednostkowymi netto określonymi w Załączniku Nr 1 do Umowy , powiększonej o wartość należnego podatku od towarów w wysokości naliczonej zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.jedn. Dz.U. z 2022 r. poz. 931 z późn.zm.) obowiązującymi w dniu wystawienia faktury. Na dzień zawarcia Umowy wynagrodzenie brutto wynosi …… PLN (słownie: ..... złotych).
2. W cenach jednostkowych, o których mowa w ust. 1, mieszczą się wszelkie koszty realizacji przedmiotu Umowy, w tym w szczególności koszty Oprogramowania,

Licencji, wdrożenia Oprogramowania, dostawy do miejsca Lokalizacji, a także inne koszty poniesione przez Wykonawcę w związku z realizacją Przedmiotu Umowy w tym koszty związane z udzieloną gwarancją.

3. Wartość wynagrodzenia określona w ust. 1 jest wartością maksymalną zamówienia.

4. Podstawę do wystawienia faktury stanowi Protokół Odbioru, o którym mowa w § 3 ust.1, podpisany przez Przedstawicieli Stron bez żadnych uwag. Zamawiający zapłaci za Przedmiot Umowy faktycznie zamówiony, spełniający wymagania jakościowe i techniczne opisane w OPZ, dostarczony do Miejsca Lokalizacji i odebrany przez Zamawiającego.
5. Wykonawca wystawi fakturę z uwzględnieniem stawki podatku VAT, w wysokości zgodnej z przepisami, o których mowa w ust.1, dla Zamawiającego:

**Samodzielny Publiczny Kliniczny Szpital Okulistyczny**
**03-709 Warszawa, ul. Józefa Sierakowskiego 13**
**NIP: 113-21-68-300**

6. Płatność należności, na podstawie faktury, o której mowa w ust. 5 zostanie dokonana przelewem, na rachunek bankowy Wykonawcy nr : ..... , potwierdzony na fakturze, w terminie 30 dni od daty otrzymania prawidłowo wystawionej faktury.
7. Zamawiający wyraża zgodę na przekazywanie faktur w postaci:
   1) papierowej – na adres Dział Księgowości SPKSO przy ul. Marszałkowskiej 24/26 w Warszawie (00-576), albo
   2) elektronicznej – w formacie pdf, na adres poczty elektronicznej: faktury@spkso.waw.pl z adresu poczty elektronicznej przedstawiciela Wykonawcy, wskazanego w § 4 ust. 2.
8. Za datę otrzymania faktury, o której mowa w ust. 5, przyjmuje się datę:
   1) dostarczenia faktury w postaci papierowej na adres wskazany w ust. 7 pkt 1) albo
   2) pojawienia się faktury w skrzynce odbiorczej pod adresem poczty elektronicznej wskazanej przez Zamawiającego w ust. 7 pkt 2), a jeżeli faktura pojawiła się w skrzynce po godz. 15.00 – następny dzień roboczy.
9. Błędnie wystawiona faktura może spowodować zawieszenie biegu terminu płatności, o którym mowa w ust. 6, do momentu dostarczenia poprawionych lub brakujących dokumentów.
10. Za datę zapłaty przyjmuje się datę uznania wpłaty dokonanej przez Zamawiającego na rachunku bankowym Wykonawcy wskazanym w fakturze.
11. Zobowiązanie Zamawiającego dotyczy należności określonej w Umowie. Jeżeli należność naliczona na fakturze wystawionej przez Wykonawcę przewyższy cenę uzgodnioną przez Strony, Zamawiający dokona zapłaty jedynie do ceny wynikającej z postanowień ust. 1, a Wykonawca zobowiązuje się do niezwłocznego wystawienia faktury korygującej.
12. Zgodnie z przepisami ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (t.j. Dz. U. z 2020 r. poz. 1666 ze zm.) Wykonawca uprawniony jest do przesłania Zamawiającemu ustrukturyzowanej faktury

elektronicznej na konto Zamawiającego za pośrednictwem Platformy Elektronicznego Fakturowania dostępnej pod adresem : www.efaktura.gov.pl.

## § 6.
## LICENCJE I GWARANCJA JAKOŚCI NA OPROGRAMOWANIE

1. Wykonawca oświadcza, że:
   1) w ramach wynagrodzenia określonego w § 5 ust. 1, udziela Zamawiającemu nieograniczonej w czasie licencji niewyłącznej na użytkowanie Oprogramowania, na warunkach producenta określonych w dokumencie Licencyjnym;
   2) Produkty objęte przedmiotem Umowy są wolne od wad fizycznych i prawnych oraz mogą być użytkowane zgodnie z przeznaczeniem, opisanym w szczególności w Rozdziale II OPZ Załączniku nr 2 do Umowy oraz spełniają wymagania co do należytej jakości i aktualności;
   3) udziela Zamawiającemu gwarancji na prawidłowe działanie Oprogramowania na okres zgodny z ze wskazanym w rozdziale VII pkt 2 OPZ, licząc od dnia podpisania bez żadnych uwag Protokołu Odbioru, o którym mowa w § 3, oraz zobowiązuje się, w ramach wynagrodzenia określonego w § 5 ust. 1, usunąć wszystkie wady, usterki i nieprawidłowości w działaniu Oprogramowania;

   4) W ramach udzielonej gwarancji zobowiązuje się zapewnić 36-o miesięczną usługę serwisową i wsparcie producenta oraz możliwość aktualizacji mechanizmów bezpieczeństwa, w tym usunąć nieodpłatnie wszystkie wady, usterki i nieprawidłowości w działaniu Oprogramowania. Naprawa powinna być dokonana w terminie nie przekraczającym ….. godzin od zgłoszenia.

   5) Okres gwarancji przedłuża się każdorazowo o liczbę dni niesprawności Oprogramowania, liczonych od dnia zgłoszenia awarii do dnia usunięcia usterek;
   6) Zamawiający ma prawo do tworzenia kopii bezpieczeństwa Oprogramowania, na własny użytek, w zakresie, w jakim jest to niezbędne do instalowania, przechowywania i korzystania z Oprogramowania;
   7) Zamawiający ma prawo do wprowadzania Produktu do pamięci komputerowych stacji roboczych i serwerów komputerowych;
   8) Zamawiający nie ma prawa udzielania dalszych sublicencji na Oprogramowanie.
2. Wykonawca gwarantuje, że w ramach Licencji, Zamawiający będzie uprawniony do dokonywania bezpłatnych Aktualizacji Oprogramowania na zasadach określonych w ogólnych warunkach producenta Oprogramowania.
3. W przypadku wadliwie działających nośników Oprogramowania Wykonawca zobowiązuje się wymienić wadliwe nośniki na nowe, wolne od wad.
4. Wszelkie koszty związane ze świadczeniem usług gwarancyjnych obciążają Wykonawcę, w szczególności koszty dojazdów, pracy serwisu, oględzin, diagnostyki, naprawy i robocizny.
5. Jakiekolwiek działanie niepożądane lub reklamacja jakościowa związana z użyciem Produktów będzie rozpatrywana zgodnie z lokalnymi przepisami prawa. Informacje o ww. zdarzeniach będą przekazywane niezwłocznie do Wykonawcy pod następujące dane :
   1) Nazwa: ……
   2) Adres: ……

3) Tel.: ……..……..……..……..
4) Fax:…….

Email: ……..…….

6. Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie terminu jej obowiązywania, jeżeli poinformował o wadzie lub usterce Wykonawcę przed upływem tego terminu.
7. W przypadku jakichkolwiek rozbieżności pomiędzy warunkami ważności gwarancji, a postanowieniami Umowy, bezwzględne pierwszeństwo mają postanowienia Umowy.
8. Zamawiającemu przysługują uprawnienia z tytułu rękojmi zgodnie z przepisami Kodeksu cywilnego, niezależnie od uprawnień z tytułu gwarancji. Bieg terminu rękojmi rozpoczyna się z dniem podpisania Protokołu Odbioru, o którym mowa w § 3 ust.1.
9. Jeżeli z powodu wady prawnej Produktów Zamawiający będzie zmuszony wydać je osobie trzeciej, Wykonawca jest obowiązany do zwrotu otrzymanego wynagrodzenia w odniesieniu do części przedmiotu Umowy, której dotyczy wada prawna, bez względu na inne postanowienia Umowy.

## § 7.

## Podwykonawcy

1. Wykonawca nie może powierzyć w całości ani w części wykonania przedmiotu Umowy osobom trzecim bez zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności, z wyjątkiem zakresu wskazanego w ofercie Wykonawcy.
2. Zgodnie z oświadczeniem zawartym w ofercie oraz według stanu obowiązującego na dzień zawarcia Umowy – Wykonawca nie powierza podwykonawcom wykonania żadnej części przedmiotu Umowy/powierza podwykonawcy(-com) wykonanie następującej części przedmiotu Umowy ……..……..…… [2]
3. Wykonawca za działania lub zaniechania podwykonawcy(-ców) ponosi odpowiedzialność jak za własne działania lub zaniechania i nie może zwolnić się od odpowiedzialności względem Zamawiającego z tego powodu, że niewykonanie lub nienależyte wykonanie Umowy przez Wykonawcę było następstwem niewykonania lub nienależytego wykonania zobowiązań wobec Wykonawcy przez jego podwykonawcę(-ców).

## § 8.

## Kary umowne

1. Strony ustalają odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy w formie kar umownych.

2. W przypadku niewykonania lub nienależytego wykonania Umowy lub jej części, Zamawiający ma prawo naliczyć Wykonawcy kary umowne w kwocie odpowiadającej:

[2] Niepotrzebne skreślić. W przypadku powierzenia podwykonawcy(-com) wykonania części przedmiotu Umowy podać dane identyfikacyjne każdego podwykonawcy, tj. nazwę i adres podwykonawcy, NIP i numer wpisu do KRS (jeżeli dotyczy) jeżeli podwykonawca(-cy) są znani w dniu zawarcia Umowy.

1) **10% wartości netto** niezrealizowanej części Umowy, w przypadku gdy Zamawiający odstąpi od Umowy lub jej części z powodu okoliczności, za które wyłączną odpowiedzialność ponosi Wykonawca;

2) **0,2% wartości netto** części przedmiotu Umowy za każdy dzień zwłoki w dostawie danej części Przedmiotu Umowy, w przypadku przekroczenia terminu określonego w § 3 ust. 1, za które wyłączną odpowiedzialność ponosi Wykonawca;

3) **0,2% wartości netto** części przedmiotu Umowy za każdy dzień zwłoki w wykonaniu naprawy lub usunięciu usterki gwarancyjnej, w przypadku przekroczenia terminu, o którym mowa odpowiednio w § 6 ust.1 zdanie drugie, za które wyłączną odpowiedzialność ponosi Wykonawca..

3. Zamawiający zapłaci Wykonawcy karę umowną, w przypadku niewywiązania się z zobowiązań umownych w kwocie odpowiadającej:

1) **10% wartości netto** niezrealizowanej przez Wykonawcę części Umowy – w przypadku gdy Wykonawca lub Zamawiający odstąpi od Umowy z przyczyn, za które wyłączną odpowiedzialność ponosi Zamawiający, z wyłączeniem przypadków określonych w § 10 ust. 1;

2) **0,2% wartości netto** części przedmiotu Umowy za każdy dzień zwłoki w dokonaniu odbioru Przedmiotu Umowy, w przypadku przekroczenia terminu określonego w § 3 ust. 5 lub 6 licząc od dnia jego dostarczenia.

4. Łączna wartość kar umownych naliczonych:

1) Wykonawcy na podstawie ust. 2 pkt 2 nie może przekroczyć 10% wartości netto przedmiotu Umowy określonej w § 5 ust. 1;

2) Wykonawcy na podstawie ust. 2 pkt 3 nie może przekroczyć 10% wartości netto przedmiotu Umowy określonej w § 5 ust. 1;

3) Zamawiającemu na podstawie ust. 3 pkt 2 – nie może przekroczyć 10% wartości netto przedmiotu Umowy określonej w § 5 ust. 1.

5. Strona, która naliczy kary umowne, wystawi drugiej Stronie notę obciążeniową, a Strona, której naliczono kary umowne, zobowiązana jest do dokonania płatności w wysokości wynikającej z noty obciążeniowej w terminie 14 dni licząc od dnia jej otrzymania.

6. Strona, która nie zgadza się z naliczeniem kary umownej, przekazuje drugiej Stronie pisemne zastrzeżenia w terminie określonym w ust. 5. Odpowiedź na zastrzeżenia i ewentualne kolejne pisma Strony przekazują sobie nawzajem każdorazowo w terminie nie dłuższym niż 7 dni od dnia otrzymania pisma, którego odpowiedź dotyczy.

7. W przypadku gdy wartość roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, przewyższa wartość przewidzianych kar umownych, Zamawiający może dochodzić odszkodowania na zasadach ogólnych.

8. Zamawiający ma prawo żądać od Wykonawcy odszkodowania na zasadach ogólnych, w przypadku niewykonania lub nienależytego wykonania przez Wykonawcę pozostałych zobowiązań wynikających z Umowy, innych niż wymienione w ust. 2.

**§ 9.**

## Zmiany Umowy

1. Zakazuje się zmian postanowień Umowy w stosunku do treści oferty, chyba, że zachodzi co najmniej jedna z okoliczności wskazanych w art. 455 Ustawy Prawo zamówień publicznych lub w ust.2.

2. Zamawiający przewiduje możliwość wprowadzenia zmian postanowień zawartej umowy w przypadku:

   a) działania siły wyższej uniemożliwiającej wykonanie przedmiotu umowy w ustalonym terminie,

   b) zmian wynikających z przepisów prawa, w tym zmiany stawki VAT.

3. W przypadku zaistnienia konieczności dokonania zmiany w zakresie opisanym w ust.2 Wykonawca przedstawi Zamawiającemu pisemny wniosek w tej sprawie. Po zaakceptowaniu go przez Zamawiającego zostanie sporządzony aneks do umowy.

4. Umowa może zostać rozwiązana w wyniku oświadczenia złożonego przez Zamawiającego skutkującego rozwiązaniem umowy bez wypowiedzenia w przypadku braku dostarczenia oprogramowania lub jeśli wykonanie umowy nie leży w interesie publicznym.

5. Wykonawca (wierzyciel) nie może bez zgody Zamawiającego (dłużnika) przenieść swoich wierzytelności na osobę trzecią, a zgody takiej Zamawiający nie może bezpodstawnie odmówić.

6. Wszelkie zmiany i uzupełnienia Umowy wymagają zachowania, pod rygorem nieważności, formy pisemnej lub elektronicznej Aneksu i muszą być dokonane przez umocowanych do tego przedstawicieli obu Stron.

## § 10.

## Forma i tryb rozwiązania Umowy

1. Niezależnie od przypadków odstąpienia od Umowy wskazanych w Kodeksie Cywilnym oraz w ustawie PZP, Zamawiającemu przysługuje prawo odstąpienia od Umowy lub jej niezrealizowanej części z ważnych powodów, w terminie 30 dni od dnia stwierdzenia ich wystąpienia przez Zamawiającego. Za ważne powody uważa się przypadki gdy:

   1) termin realizacji Przedmiotu Umowy, o którym mowa w § 3 ust. 1, zostanie przekroczony o więcej niż **10 dni** z powodu okoliczności leżących wyłącznie po stronie Wykonawcy;

   2) Zamawiający stwierdzi wady fizyczne lub prawne Oprogramowania, a Wykonawca nie usunie ich w wyznaczonym przez Zamawiającego terminie;

   3) Wykonawca powierzył wykonanie Umowy osobie trzeciej lub rozszerzył zakres podwykonawstwa poza wskazany w ofercie bez zgody Zamawiającego i nie zmienił sposobu realizacji Umowy mimo wezwania go do tego przez Zamawiającego w terminie określonym w tym wezwaniu;

   4) Wykonawca nie realizuje przedmiotu Umowy zgodnie z Umową lub nienależycie wykonuje swoje zobowiązania Umowne i nie zmienił sposobu realizacji Umowy mimo wezwania go do tego przez Zamawiającego w terminie określonym w tym wezwaniu.

2. Wykonawcy przysługuje prawo odstąpienia od Umowy w przypadku gdy Zamawiający w sposób zawiniony nienależycie wykonuje swoje zobowiązania umowne, co Wykonawca jest w stanie wykazać za pomocą stosownych dowodów, i nie zmienił sposobu realizacji Umowy mimo wezwania go do tego przez Wykonawcę, w terminie określonym w tym wezwaniu.
3. Poza przypadkami, o których mowa w ust. 1 i 2, żadnej ze Stron nie przysługuje prawo odstąpienia od niniejszej Umowy lub wypowiedzenia niniejszej Umowy przed upływem okresu jej obowiązywania.
4. Odstąpienie od Umowy lub jej niezrealizowanej części wymaga złożenia oświadczenia w formie pisemnej pod rygorem nieważności i jest skuteczne z dniem doręczenia tego oświadczenia drugiej Stronie.
5. Oświadczenie o odstąpieniu od Umowy winno zostać przekazane przedstawicielowi drugiej Strony za pokwitowaniem lub winno zostać złożone w siedzibie Strony lub przesłane listem poleconym na adres siedziby Strony wskazany w komparycji Umowy. Korespondencję odebraną, lub nieodebraną a nadaną listem poleconym za pośrednictwem operatora wyznaczonego i zwróconą nadawcy z powodu braku możliwości jej doręczenia, uważa się za skutecznie doręczoną.
6. W przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn wskazanych w ust. 1, Wykonawca ma prawo do wynagrodzenia wyłącznie za część przedmiotu Umowy zrealizowaną zgodnie z Umową do dnia złożenia przez Zamawiającego oświadczenia o odstąpieniu od Umowy.
7. W przypadku rozwiązania Umowy przez którąkolwiek ze Stron, Zamawiający zobowiązuje się w terminie do 30 dni od daty otrzymania prawidłowo wystawionej faktury pokryć koszty części przedmiotu Umowy zrealizowanej zgodnie z Umową do dnia rozwiązania Umowy. Postanowienia § 5 stosuje się odpowiednio.

## § 11.
## Postanowienia końcowe

1. Wykonawca nie może przekazać praw i obowiązków wynikających z niniejszej Umowy na rzecz osób trzecich bez zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności.
2. Wykonawca jest zobowiązany do informowania Zamawiającego o zmianie formy prawnej prowadzonej działalności, o wszczęciu postępowania układowego lub upadłościowego oraz zmianie jego sytuacji ekonomicznej mogącej mieć wpływ na realizację Umowy oraz o zmianie siedziby firmy pod rygorem skutków prawnych wynikających z zaniechania, w tym do uznania za doręczoną korespondencję skierowaną na ostatni adres podany przez Wykonawcę.
3. Specyfikacja Warunków Zamówienia i Oferta Wykonawcy stanowią integralną część niniejszej Umowy.
4. Strony postanawiają, iż w przypadku jakichkolwiek wątpliwości poszczególne postanowienia Umowy będą interpretowane w taki sposób, aby były zgodne z obowiązującymi przepisami oraz intencją Stron.
8. W przypadku gdyby którekolwiek z postanowień niniejszej Umowy zostało uznane za niezgodne z prawem, nieważne lub okazało się niewykonalne, postanowienie takie

będzie uważane za niezastrzeżone w Umowie, przy czym wszystkie dalsze postanowienia Umowy pozostają w mocy. Postanowienie uznane za niezgodne z prawem, nieważne lub niewykonalne zostanie zastąpione postanowieniem o podobnym znaczeniu, w tym przede wszystkim o treści odzwierciedlającej pierwotne intencje Stron w granicach dopuszczalnych przez prawo.

9. Wszelkie spory mogące wyniknąć pomiędzy Stronami przy realizowaniu przedmiotu Umowy lub z nią związane, w przypadku braku możliwości ich polubownego rozwiązania, będą rozpatrywane przez sąd właściwy dla siedziby Zamawiającego.
10. Niezależnie od wygaśnięcia lub rozwiązania niniejszej Umowy z dowolnej przyczyny, prawa i obowiązki każdej ze Stron wynikające z postanowień Umowy, będą w pełni obowiązywać na zasadach określonych w Umowie w zakresie:
    1) zobowiązania Wykonawcy z tytułu gwarancji jakości i rękojmi za wady oraz licencji, o których mowa w **§ 6**, w odniesieniu do części przedmiotu Umowy, której wykonanie uznano za należyte i zgodne z Umową i za którą Zamawiający zapłacił Wykonawcy wynagrodzenie zgodnie z § 10 ust. 7;
    2) kar umownych związanych z niewykonaniem lub nienależytym wykonaniem Umowy lub jej części, o których mowa w § 8.
11. Wszystkie dokumenty wymienione w niniejszej Umowie, zarówno nazwane jak i nienazwane załącznikami, stanowią integralną część Umowy.
12. Niniejsza Umowa obowiązuje od dnia zawarcia, co oznacza dzień złożenia podpisu przez ostatnią ze Stron.

Niniejszą umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego jeden dla Wykonawcy.

| | |
|---|---|
| ..... | ..... |
| za Wykonawcę | za Zamawiającego |

**Załącznik Nr 1**

do Umowy nr SPKSO/ZP- ……/2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

# FORMULARZ ASORTYMENTOWO-CENOWY

**Załącznik Nr 2**

do Umowy nr SPKSO/ZP- ……/2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

# OPIS PRZEDMIOTU ZAMÓWIENIA

**PAKIET NR 1 – Dostawa licencji i oprogramowania wraz z wdrożeniem**

**Przedmiotem zamówienia jest zakup licencji oprogramowania zwiększającego bezpieczeństwo i wdrożenie na potrzeby i na podstawie „ZARZĄDZENIE NR 117/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 września 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców".**

## I. Przedmiot zamówienia:

1. **Zakup licencji oraz wdrożenie centralnego systemu ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania - XDR.**
2. **Zakup i wdrożenie oprogramowania kontroli dostępu i zarządzania tożsamościami użytkowników oraz dostępu komputerów do sieci lokalnej.**

## II. Wymagane funkcjonalności

**ZAKUP LICENCJI ORAZ WDROŻENIE CENTRALNEGO SYSTEMU OCHRONY ENDPOINT Z MODUŁEM ROZSZERZONEGO WYKRYWANIA I REAGOWANIA – XDR:**

**Zamawiający wykorzystuje obecnie UTM firmy Sophos XG ze wsparciem do 11 listopada 2025r. Zamawiający wymaga, aby dostarczone oprogramowanie posiadało licencje wieczyste ze wsparciem technicznym min. 36 miesięcy oraz żeby było w pełni kompatybilne z posiadanym zarządzanym urządzeniem UTM Sophos XG.**

1. Rozwiązanie musi mieć możliwość ochrony komputerów z systemem Windows (8 i nowsze) oraz serwerów z systemem Windows Server (Windows Server 2012 i nowsze).
2. Rozwiązanie musi umożliwiać stosowanie wielu polityk bezpieczeństwa.
3. Rozwiązanie musi posiadać zarządzalny mechanizm aktualizacji.
4. Rozwiązanie musi zapewniać kategoryzowanie i blokowanie stron.
5. Rozwiązanie musi zapewniać ochronę urządzeń przenośnych (np., USB).
6. Rozwiązanie musi posiadać skaner antymalware oraz kontrolę aplikacji.
7. Rozwiązanie musi posiadać ochronę przed włamaniami (IPS) oraz ochronę przed włamaniami opartą na hostach (HIPS).
8. Rozwiązanie musi oferować ochronę w czasie rzeczywistym.
9. Rozwiązanie musi być rozbudowane o opcję PUA – Blokowanie potencjalnie niechcianych aplikacji.
10. Rozwiązanie musi chronić Zamawiającego przed utratą danych (DLP).
11. Rozwiązanie musi zapewniać zgodność z interfejsem skanowania antymalware AMSI.
12. Rozwiązanie musi wykrywać złośliwy ruch [MTD].
13. Rozwiązanie musi posiadać ochronę przed eksploitami, zmianami w kodzie aplikacji oraz przez ransomware.
14. Rozwiązanie musi posiadać ochronę sektora rozruchowego dysku oraz ochronę przed atakami Man-in-the-Browser.
15. Rozwiązanie musi oferować wykrywanie zagrożeń powiązanych ze sobą procesami.
16. Rozwiązanie musi oferować wykrywanie podejrzanych zdarzeń i priorytetyzację, a także analizę zagrożeń w modelu drzewa.

17. Rozwiązanie musi oferować automatyczne usuwanie malware i izolację zarażonego hosta na żądanie.
18. Rozwiązanie musi gwarantować przechowywanie danych w chmurze do dalszej analizy, a także zdalny dostęp do centralnej konsoli zarządzającej w celu przeprowadzenia śledztwa i usunięcia problemu
19. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
20. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
21. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do systemu graylog (syslog).
22. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych
1. Rozwiązanie musi wspierać systemy operacyjne Windows dla systemów Windows 8 i nowszych: (Windows 8/Windows 10/Windows 11).
2. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
3. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
5. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
6. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
7. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
8. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
9. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
10. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
11. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

14. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

15. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

16. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

17. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

18. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

19. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

20. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

21.Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
22. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
23. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
24. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
25. Rozwiązanie musi zapewniać ochronę przed zagrożeniami zero-day.
26. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

**Dodatkowe wymagania dla ochrony serwerów Windows:**

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 8/8.1/10 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Extended Detection and Response**

1. Rozwiązanie musi posiadać moduł XDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.

2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.

3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica".

6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.

7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.

10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.

**ZAKUP I WDROŻENIE OPROGRAMOWANIA KONTROLI DOSTĘPU I ZARZĄDZANIA TOŻSAMOŚCIAMI UŻYTKOWNIKÓW ORAZ DOSTĘPU KOMPUTERÓW DO SIECI LOKALNEJ.**

**I. Zamawiający wykorzystuje obecnie:**
**- przełączniki dostępowe (4szt. Aruba 2930F 48G POE+ 4SFP+ JL256A);**

**- przełącznik zarządzalne przy urządzeniach końcowych (61szt. TP-LINK SG-105E oraz TP-LINK SG-108E).**

**- kompletny punkt sieci bezprzewodowej (15 szt. Aruba AP-515 (RW) Unified AP Q9H62A) wraz z punktem centralnego zarządzania Aruba AirWave.**

**Zamawiający wymaga, aby dostarczone oprogramowanie było w pełni kompatybilne z wymienionymi urządzeniami.**

**II. Minimalne wymagania sprzętowe**

1. System musi bazować na standardach RADIUS oraz TACACS+.
1.1 System powinien oferować różne możliwości zastosować, szczególnie:
- autoryzację bezprzewodową i przewodową w sieciach korporacyjnych,
- realizację dostępu dla gości,
- realizację dostępu BYOD (Bring Your Own Device),
- wymuszanie polityk bezpieczeństwa dla użytkowników lokalnych i mobilnych.
2. System musi umożliwiać instalację w środowisku Vmware (ESXi 7).
3. System musi posiadać licencje dostępową pozwalającą równoczesną obsługę co najmniej 250 urządzeń końcowych oraz licencje Onboard pozwalającą na realizację usługi BYOD w sieciach korporacyjnych dla co najmniej 150 urządzeń.

**III. Funkcjonalności**

1. System musi posiadać element funkcjonalny zarządzania, umożliwiający administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji sytemu oraz jego monitorowanie
1.1. System musi posiadać element funkcjonalny logowania i rozwiązywania problemów, umożliwiający gromadzenie wiadomości logowania z:
- infrastruktury sieciowej, w tym przełączników dostępowych
- sesji uwierzytelniania 802.1X
- zdarzeń kontroli dostępu (autoryzacji)
- zdarzeń głębokiej analizy stacji (posture assessment)
- zdarzeń związanych z błędami
- zdarzeń związanych z alarmami systemowymi
1.2. System musi posiadać element funkcjonalny usługowy (Policy Service), realizujący funkcje:
- serwera RADIUS dla infrastruktury sieciowej
- serwera polityk uwierzytelniania i kontroli dostępu 802.1X
- elementu decyzyjnego dla głębokiej analizy stacji (posture assessment)
- serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego (Guest Auth) i uwierzytelniania webowego (WebAuth)
- usług do profilowania stacji końcowych (Profiler)

2. System musi wspierać protokół Windows Active Directory
3. System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową.
4. System musi co najmniej wspierać następujące protokoły uwierzytelniania:

- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
- EAP-MS-CHAPv2
- EAP-GTC
- EAP-TLS

5. System musi umożliwiać konfigurację mechanizmów EAP-TLS Session Resume i PEAP Session Timeout.
6. System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect.
7.System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego.
8.System musi umożliwiać tworzenie kopii zapasowej systemu.
9.System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
10.System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów.
11.System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
- dostęp do interfejsu konfiguracji usług tożsamości 802.1X
- dostęp do interfejsu konfiguracji urządzeń sieciowych
- dostęp do interfejsu konfiguracji polityk
- dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
- dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania

12.System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
13.System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
- wiadomości e-mail
- syslog/graylog

14.System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
- nazwy użytkownika
- adresu MAC
- Audit Session ID
- adresu IP NAS
- numeru portu NAS
- statusu uwierzytelnienia (udana lub nieudana)
- powodu, jeżeli uwierzytelnienie nieudane
- zakresu czasowego co do dnia, godziny i minuty

15.System musi umożliwiać uwierzytelnienie i kontrolę dostępu:
- kablowego w sieci LAN
- bezprzewodowego w sieci WLAN
- zdalnego VPN

16.System musi wspierać implementację 802.1X przynajmniej z wbudowanym klientem 802.1X dla Windows 8/10
17.System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).
18.System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
19.System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV.
20.System musi posiadać lokalną bazę stacji końcowych. Lokalną bazę stacji końcowych można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC.
21.System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej Google Chrome, Mozilla Firefox.
22.System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby.

23.System musi umożliwiać konfigurację wyglądu portalu dostępu dla gościa, w tym:
- zmianę logo strony logowania;
- zmianę obrazu tła strony logowania;
- zmianę logo bannera;
- zmianę obrazu tła bannera;
- zmianę koloru tła strony logowania;
- zmianę koloru tła strony bannera;
- zmianę koloru tła strony z treścią;
- zresetowanie ustawień do konfiguracji fabrycznej producenta.
24.System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP oraz HTTPS.
25.System musi umożliwiać zmianę adresu URL strony dostępowej dla gościa.
26.System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych na żądanie oraz okresowo co zadaną liczbę dni i o określonej godzinie.
27.System musi umożliwiać wyświetlenie czasu: ostatniego kasowania wygasłych kont gościnnych oraz następnego kasowania wygasłych kont gościnnych.
28.System musi umożliwiać stworzenie własnego wzorca językowego portalu dostępowego.
29.System musi umożliwiać specyfikację opcjonalną lub obowiązkową danych gościa w trakcie próby logowania.
30.System musi wyświetlać gościom informację o akceptacji polityki akceptowalnego użycia sieci (AUP).
31.System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego w przedziale od 1 do 9.
32.System musi umożliwiać konfigurację czasu ważności hasła.
33.System musi umożliwiać kreację profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego.
34.System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych.
35.System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego.
36.System musi umożliwiać dokonanie profilowania (profiling) stacji końcowej i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
37.System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł: DHCP, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMP.
38.System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
39.System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym minimum dla:
- Android;
- Apple: Apple MacBook, Apple iPad, Apple iPhone, Apple iPod;
- Microsoft Workstation: Windows 7, Windows 8, Windows 10, Windows 11;
40.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows 11 pod kątem wpisów w rejestrze, w tym kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem.
41.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem uruchomionych aplikacji (Application Condition).
42.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem zainstalowanych aplikacji Antywirusowych w tym:
- stwierdzenia czy system AV jest obecny na stacji;
- stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni;
- daty ostatniego pliku definicji;
- aktualnego czasu systemowego.
43.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem zainstalowanych aplikacji AntiSpyware w tym:
- stwierdzenia czy system AS jest obecny na stacji;

- stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni;
- daty ostatniego pliku definicji;
- aktualnego czasu systemowego.

**IV. Raportowanie**

System musi umożliwiać generowanie przynajmniej następujących raportów:
- raportów dla protokołów AAA;
- accountingu RADIUS;
- uwierzytelniania RADIUS;
- raportów dozwolonych protokołów;
- sumarycznej informacji o uwierzytelnieniach RADIUS per protokół;
- raportów dla poszczególnych instancji serwerów systemu, w tym:
    a) administratorów systemu i ich uprawnień (administrator entitlements);
    b) logowania administratorów do systemu;
    c) zmian konfiguracji serwera dokonanych przez administratorów;
    d) zdrowia serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS);
    e) zmian operacyjnych serwera dokonanych przez administratorów;
- raportów dla stacji końcowych, w tym:
    a) Top N uwierzytelnień per adres MAC stacji;
    b) Top N uwierzytelnień per użytkownik;
    c) działań podsystemu profilera per adres MAC;
    d) zarejestrowane urządzenia per użytkownik;
- raportów dla błędów, w tym:
    a) błędów uwierzytelniania per szczegółowy kod błędu który wystąpił;
    b) sumarycznych przyczyn nieudanych uwierzytelnień;
    c) Top N uwierzytelnień per rodzaj błędu;
- raportów dla urządzeń sieciowych:
    a) sumarycznych uwierzytelnień dla urządzeń sieciowych;
    b) Top N uwierzytelnień per urządzenie sieciowe;
    c) niedostępności serwera AAA dla urządzenia sieciowego;
    d) wiadomości logowanych przez urządzenia sieciowe;
    e) stanu portów i sesji urządzenia sieciowego z perspektywy SNMP;
    f) top N niedostępności serwera AAA dla urządzeń sieciowych;
- raportów użytkowników;
- raportów katalogu sesji, m.in. aktywnych sesji RADIUS, historii sesji RADIUS, zaterminowanych sesji RADIUS.

**V. Organizacja wdrożenia**

1.Przeprowadzenie analizy przedwdrożeniowej i uzgodnienie z Zamawiającym harmonogramu wdrożenia.
2.Dostarczeniu licencji Systemu.
3.Instalacja i konfiguracja Systemu (w tym prace konfiguracyjne systemu uwierzytelniania opartego o protokół PEAP z protokołem EAP-TLS w wersji 802.1x oraz konfiguracja Captive Portal z autentyfikacją opartą na Self-registration.
4.Dostawca sprawdzi i dostosuje oprogramowanie na przełącznikach Zamawiającego do wersji zalecanej przez producenta systemu NAC.
5.Zamawiający wymaga, aby wraz z rozwiązaniem oraz kontraktem serwisowym oferta obejmowała minimum 2 dniowy instruktaż powdrożeniowy dla 3 pracowników Zamawiającego obejmujące zakresem obsługę systemu NAC. Warsztaty muszą być przeprowadzone w siedzibie Zamawiającego lub za pomocą platformy umożlwiającej zdalne prowadzenie szkoleń.
6.Przeprowadzenie szkoleń.
7.Dostarczenie dokumentacji powykonawczej.

## VI. Wymagania dodatkowe

1. Całość oprogramowania musi zostać dostarczona i uruchomiona w siedzibie Zamawiającego.
2. Oferowane rozwiązanie musi być produktem fabrycznie nowym.
3. Oferowane rozwiązanie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub ze sprzedaży.
4. Zamawiający wymaga zapewnienia Wykonawcy, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
5. Wykonawca zobowiązuje się do wykonania wszelkich prac z zachowaniem najwyższej staranności.
6. Dostawca musi dostarczyć wszystkie niezbędne komponenty do wdrożenia.
7. Wdrożenie musi zakończyć wykonanie testów poprawności pracy systemu kontroli dostępu do sieci oraz sporządzenie protokołu odbioru.
8. Dostawca rozwiązania musi zatrudniać minimum 1 inżyniera wsparcia technicznego posiadającego techniczny certyfikat producenta w ścieżce Security (np. CCIE Security lub równoważny).
9. Zamawiający wymaga wdrożenia najnowszej, dostępnej wersji systemu NAC wspieranej przez producenta systemu.

## VII. Wymagania obsługi serwisowej

1. Oferowane rozwiązanie musi posiadać bezterminową (dożywotnią) licencję.
2. Oferowane rozwiązanie musi posiadać 36-miesięczną usługę serwisową, gwarancję i wsparcie producenta oraz możliwość aktualizacji mechanizmów bezpieczeństwa.
3. W czasie obowiązywania usługi serwisowej, Zamawiający musi mieć prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade) na posiadanej przez siebie platformie.
4. W czasie obowiązywania usługi serwisowej Zamawiający musi mieć dostęp do wsparcia technicznego producenta lub autoryzowanego partnera producenta, świadczonego w dni robocze od poniedziałku do piątku w godzinach 9:00-17:00.
5. Zamawiający może zgłaszać sprawy z zakresu pomocy technicznej kontaktując się poprzez dedykowany adres email lub numer infolinii.
6. Dostarczone oprogramowanie musi posiadać gwarancję producenta na cały czas obowiązywania usługi serwisowej.
7. Dokumentacja do systemu zarządzania musi być publicznie dostępna na stronie internetowej producenta.
8. Producent musi publikować na swojej stronie internetowej informacje o wykrytych lukach bezpieczeństwa w systemie.

**Załącznik Nr 3**

do Umowy nr SPKSO/ZP- ...../2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

# PROTOKÓŁ ODBIORU

W dniu ..... dokonano odbioru systemu, wdrożenia oprogramowania oraz szkolenia personelu Zamawiającego na podstawie Umowy nr ..... z dnia ....., zawartej pomiędzy:
Wykonawcą – .....

a Zamawiającym - Samodzielnym Publicznym Klinicznym Szpitalem Okulistycznym w Warszawie, ul. Sierakowskiego 13, 03-709 Warszawa.

**Przedmiot umowy/przekazania/odbioru obejmuje w szczególności:**

3) centralny system ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania - XDR .....;
4) system zarządzania dostępem użytkowników i urządzeń do sieci .....;
5) prace wdrożeniowe w zakresie instalacja i konfiguracji systemów (w tym prace konfiguracyjne systemu uwierzytelniania opartego o protokół PEAP z protokołem EAP-TLS w wersji 802.1x oraz konfiguracja Captive Portal z autentyfikacją opartą na Self-registration);
6) instruktaż powdrożeniowy dla 3 pracowników Zamawiającego obejmujący zakresem obsługę wdrożonych systemów.

Zamawiający nie wnosi zastrzeżeń co do zakresu, jakości i terminowości wykonanej dostawy*.

Zamawiający wnosi następujące zastrzeżenia*:

.....
..... *- niepotrzebne skreślić

**Podpisy osób biorących udział w czynnościach odbioru przedmiotu umowy:**

Ze strony Zamawiającego:

..... - .....
(imię i nazwisko) (podpis)

Ze strony Wykonawcy:

..... - .....
(imię i nazwisko) (podpis)

**Załącznik Nr 4**

do Umowy nr SPKSO/ZP- ……/2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

# OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI INFORMACJI I DANYCH

W związku z wykonywaniem Umowy nr ..... z dnia ……. zobowiązuję się do:

1. zachowania w ścisłej tajemnicy wszelkich informacji technicznych, technologicznych, prawnych i organizacyjnych dotyczących systemów i sieci informatycznych/ teleinformatycznych oraz danych osobowych, uzyskanych w trakcie wykonywania umowy niezależnie od formy przekazania tych informacji i ich źródła;

2. wykorzystania informacji jedynie w celach określonych ustaleniami umowy oraz wynikającymi z prawnych uregulowań obowiązujących w Rzeczpospolitej Polskiej i Unii Europejskiej;

3. podjęcia wszelkich niezbędnych kroków dla zapewnienia, aby informacje poufne, wrażliwe i stanowiące tajemnicę organizacji nie zostały ujawnione w zakresie treści ani ich źródła, zarówno w całości jaki i w części osobom trzecim (nieupoważnionym) bez uzyskania uprzednio wyrażonej przez Zamawiającego pisemnej zgody, której zakres lub źródło informacji dotyczy;

4. ujawnienia informacji jedynie tym osobom, którym są one niezbędne do wykonywania powierzonych im czynności polegających na obsłudze informatycznej/ teleinformatycznej lub utylizacji nośników danych Zamawiającego i tylko w zakresie w jakim odbiorca informacji musi mieć do nich dostęp dla celów realizacji przedmiotu umowy;

5. niekopiowania, niepowielania ani – w jakikolwiek inny sposób nierozpowszechniania jakiejkolwiek informacji, o której mowa w pkt 3, chyba że do celów związanych z realizacją umowy występują uzasadnione potrzeby, po uprzednio wyrażonej przez Zamawiającego pisemnej zgody, której zakres lub źródło informacji dotyczy.

Oświadczam, że znana jest mi treść niżej wymienionych przepisów w zakresie ochrony informacji oraz odpowiedzialności za jej ujawnienie:

1. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. 2022 r., poz. 1138 t.j. z późn. zm.),
2. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
3. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 t.j.).

Wykaz osób upoważnionych przez Wykonawcę do dostępu do informacji poufnych dla celów realizacji przedmiotu umowy:

| Lp. | Imię i nazwisko | Stanowisko, nazwa i adres firmy | Podpis |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

.....

*data i podpis pełnomocnego przedstawiciela wykonawcy*

## Załącznik Nr 5

do Umowy nr SPKSO/ZP- ……/2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

# KLAUZULA INFORMACYJNA

## INFORMACJA
## o przetwarzaniu Pani/Pana danych osobowych

Zgodnie z art, 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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, zwanego dalej „RODO", informujemy, że będziemy przetwarzać Pani/Pana dane osobowe. Szczegóły tego dotyczące:

### I. Administrator danych osobowych

Samodzielny Publiczny Kliniczny Szpital Okulistyczny z siedzibą w Warszawie ul. Sierakowskiego 13, 03-709 Warszawa, działający tymczasowo pod adresem : ul. Marszałkowska 24/26 00-576 Warszawa - tel ……., informuje, że jest Administratorem Pani/Pana danych osobowych.

### III Inspektor Ochrony Danych

Administrator wyznaczył Inspektora Ochrony Danych, z którym może Pani/Pan skontaktować się w sprawach ochrony swoich danych osobowych i realizacji swoich praw za pomocą adresu e-mail: …… lub numeru telefonu: …… lub pisemnie na adres tymczasowego działania Administratora : ul. Marszałkowska 24/26 00-576 Warszawa.

### III. Cele i podstawy przetwarzania

Przetwarzanie Pani/Pana danych osobowych ma na celu:

a) przeprowadzenie i rozstrzygnięcie postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest dostawa oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT do Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie w ramach umowy o finansowanie ze środków pochodzących z funduszu przeciwdziałania COVID-19 w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców , zwanego dalej „zamówieniem publicznym" — podstawa z art. 6 ust. 1 lit. c RODO — dotyczy osób wskazanych w pkt IV lit. b.

b) wykonanie postanowień umowy w sprawie zamówienia publicznego zawartej pomiędzy Administratorem a wykonawcą — podstawa z art. 6 ust. 1 lit. f RODO dotyczy osób wskazanych do kontaktu w celu realizacji umowy, o których mowa w pkt IV lit. A.

### IV. Kategorie Pani/Pana danych, które przetwarzamy:

Będziemy przetwarzać Pani/Pana:[3]

a) imię i nazwisko, numer telefonu, adres e-mail — dotyczy osób wskazanych do kontaktu w ramach postępowania o udzielenie zamówienia publicznego lub na potrzeby wykonania umowy w sprawie zamówienia publicznego,

[3] Wykonawca przekazujący niniejszą informację w imieniu Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego osobom fizycznym, których dane udostępnił, wskazuje zakres udostępnionych danych w odniesieniu do osoby, której przekazywana jest informacja.

b) imię i nazwisko, numer telefonu, adres e-mail oraz dane indentyfikacyjne (np. numer NIP, PESEL, numer dowodu osobistego, data urodzenia — jeżeli zostały przekazane przez uczestnika postępowania o udzielenie zamówienia publicznego) — dotyczy:
— osób uprawnionych do reprezentowania wykonawcy lub podwykonawców,

## V. Odbiorcy danych

Pani/Pana dane osobowe mogą zostać udostępnione:

a) podmiotom uprawnionym do otrzymania Pani/Pana danych na podstawie obowiązujących przepisów prawa — w tym dane osobowe zawarte w dokumentacji postępowania o udzielenie zamówienia publicznego zgodnie z art. 96 ust. 3 w zw. z art. 8 ust. 1 ustawy Prawo zamówień publicznych oraz dane osobowe zawarte w umowie zgodnie z przepisami o dostępie do informacji publicznej,
b) podmiotom przetwarzającym, które świadczą nam usługi prawnicze, wspierają nas systemami teleinformatycznymi oraz dostarczają nam i obsługują nasze systemy informatyczne oraz oprogramowanie wykorzystywane do właściwej realizacji zadań Administratora.

## VI. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

Nie przekazujemy Pani/Pana danych poza teren Europejskiego Obszaru Gospodarczego.

## VII. Okres przechowywania danych

Pani/Pana dane osobowe — wskazane w dokumentacji postępowania o udzielenie zamówienia publicznego — będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia publicznego, zgodnie z obowiązującymi przepisami ustawy Prawo zamówień publicznych.

Pani/Pana dane osobowe —wskazane w umowie w sprawie zamówienia publicznego — będą przechowywane przez okres 5 lat od początku roku następującego po roku obrotowym, w którym zakończono wykonanie umowy, zgodnie z obowiązującymi przepisami o rachunkowości.

Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji zadań wynikających z celów wskazanych w pkt III, a następnie, jeśli chodzi o materiały archiwalne, zgodnie z Instrukcją Kancelaryjną SPKSO opracowaną na podstawie przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

## VIII. Pani/Pana prawa

Przysługuje Pani/Panu:

a) prawo dostępu do Pani/Pana danych osobowych — uzyskania od Administratora potwierdzenia, czy przetwarzane są Pani/Pana dane osobowe, a jeżeli ma to miejsce, uzyskanie dostępu do nich oraz przekazania Pani/Panu informacji w zakresie wskazanym w art. 15 RODO,
b) prawo do sprostowania Pani/Pana danych osobowych — żądania od Administratora niezwłocznego sprostowania danych osobowych, które są nieprawidłowe oraz uzupełnienia niekompletnych danych osobowych zgodnie z art. 16 RODO, przy czym Pani/Pana żądanie nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą umowy w zakresie niezgodnym z ustawą Prawo zamówień publicznych,
c) prawo do usunięcia Pani/Pana danych osobowych — żądania od Administratora niezwłocznego usunięcia danych osobowych, jeżeli spełniona zostanie jedna z przesłanek określonych w art. 17 RODO, m.in. dane osobowe nie są już niezbędne do celów, w których zostały zebrane, przy czym prawo usunięcia danych może zostać ograniczone ze względu na obowiązki Administratora wynikające z obowiązującego prawa,

d) prawo do ograniczenia przetwarzania Pani/Pana danych osobowych w przypadkach wskazanych w art. 18 RODO, m. in. kwestionowania prawidłowości danych osobowych, przy czym Pani/Pana żądanie nie będzie ograniczać przetwarzania Pani/Pana danych do czasu zakończenia postępowania o udzielenie zamówienia publicznego,

e) prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych (dotyczy osób wskazanych w pkt IV lit. a) — prawo sprzeciwu wobec przetwarzania Pani/Pana danych osobowych w przypadkach określonych w art. 21 RODO,

f) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych lub innego właściwego organu nadzorczego zajmującego się ochroną danych osobowych zgodnie z art. 77 RODO.

W celu skorzystania z w/w, praw należy skierować żądanie do Administratora Danych Osobowych lub Inspektora Ochrony Danych — dane kontaktowe wskazano w pkt I lub II niniejszej informacji. Proszę pamiętać, że przed realizacją Pani/Pana uprawnień Administrator będzie musiał upewnić się, ze Pani/Pan ma powyższe prawo, czyli odpowiednio Panią/Pana zidentyfikować oraz żądać dodatkowych informacji precyzujących Pani/Pana żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.

## IX. Informacja o źródle danych

Pani/Pana dane uzyskaliśmy od uczestnika postępowania o udzielenie zamówienia publicznego, tj. od ..... prowadzące/j/go/ działalność gospodarczą pod firmą **……,** adres wykonywania działalności gospodarczej: ……[4]

Ponadto Pani/Pana dane możemy pozyskiwać z publicznie dostępnych rejestrów, takich jak Centralna Ewidencja i Informacja o Działalności Gospodarczej lub Krajowy Rejestr Sądowy — jeżeli Pani/Pana dane są dostępne w tych rejestrach — dotyczy osób wymienionych w pkt IV lit. b niniejszej informacji.

## X. Informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu

Pani/Pana dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

[4] Dane wykonawcy udostępniającego Samodzielnemu Publicznemu Klinicznemu Szpitalowi Okulistycznemu dane osób fizycznych inne niż dotyczące bezpośrednio wykonawcy.

**Załącznik Nr 6**

do Umowy nr SPKSO/ZP- ...../2022 na dostawę oprogramowania oraz usług teleinformatycznych podnoszących poziom bezpieczeństwa systemów IT Samodzielnego Publicznego Klinicznego Szpitala Okulistycznego w Warszawie, realizowanej w wykonaniu Umowy z NFZ **(PAKIET NR 1)**

**Umowa powierzenia przetwarzania danych osobowych**
zawarta dnia ..... r. pomiędzy:
(zwana dalej „Umową")

**Samodzielnym Publicznym Klinicznym Szpitalem Okulistycznym (SPKSO)** z siedzibą w Warszawie przy ul. Sierakowskiego 13, 03-709 Warszawa,

reprezentowanym przez:
prof. dr. hab. n. med. Jacka Szaflika – dyrektora szpitala

zwanym w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

oraz
**Firmą .....**
reprezentowaną przez:
.....
.....
zwanym w dalszej części umowy **„Podmiotem przetwarzającym"** lub ,,Procesorem"

Administrator oraz Podmiot przetwarzający zwani są w dalszej części Umowy również Stronami.

**PREAMBUŁA**

**Zważywszy, że Strony wiąże umowa z dnia 23 ..... r. w sprawie ..... , zwane w dalszej części niniejszej Umowy ,,Umową główną", oraz, że w związku z wejściem w życie z dniem 25 maja 2018 r. 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 (RODO), następuje konieczność zawarcia umowy o powierzeniu przetwarzania danych osobowych, Strony zgodnie postanawiają, co następuje.**

**§ 1**
**Powierzenie przetwarzania danych osobowych**

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem" lub ,,RODO") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia oraz innych powszechnie obowiązujących aktów prawnych w tym zakresie. Podmiot przetwarzający oświadcza, iż powierzone przez Administratora dane osobowe będzie przetwarzał zgodnie z prawem oraz należytą starannością z uwzględnieniem zawodowego charakteru działalności prowadzonej przez Podmiot przetwarzający.
4. Administrator i Podmiot Przetwarzający oświadczają, iż dane osobowe przetwarzają przy pomocy środków technicznych i organizacyjnych spełniających wymogi określone w Rozporządzeniu.

## §2
## Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał dane osobowe w zakresie niezbędnym do prawidłowego wykonania umowy głównej.

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu należytej realizacji przedmiotu umowy głównej. Charakter przetwarzania danych przez Procesora określają jego obowiązki wynikające z umowy głównej, polegające w szczególności na :

   a) wdrożeniu centralnego systemu ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania – XDR;

   b) wdrożeniu oprogramowania kontroli dostępu i zarządzania tożsamościami użytkowników oraz dostępu komputerów do sieci lokalnej;

   c) obsłudze serwisowej wdrożonych rozwiązań.

3. Podmiot przetwarzający będzie przetwarzał następujące rodzaje danych (kategorie osób, których dane dotyczą), które Administrator powierza Procesorowi: imię i nazwisko, PESEL, numer telefonu, adres e-email, adres zamieszkania, miejsce pracy, zawód, obywatelstwo, tytuł naukowy pracowników i osób współpracujących z Administratorem na innej podstawie niż umowa o pracę oraz dane osobowe pacjentów, w tym: nazwiska i imiona, PESEL, numer telefonu, adres e-mail.

4. Przetwarzanie danych osobowych w oparciu o niniejszą Umowę odbywa się w zakresie operacji lub zestawach operacji wykonywanych na danych osobowych, tj. zbieranie, dostęp, przechowywanie oraz ich modyfikowanie – za zgodą osoby, której dane osobowe dotyczą za zgodą Administratora, bądź na polecenie Administratora.

5. Przetwarzanie, o którym mowa w ust. 2 będzie odbywać się będzie w formie elektronicznej.

6. W celu uniknięcia jakichkolwiek wątpliwości, Strony zgodnie ustalają, iż z tytułu zawarcia i realizacji niniejszej Umowy, Procesorowi nie przysługuje jakiekolwiek wynagrodzenie.

7. Podmiot przetwarzający nie może przetwarzać innych danych osobowych poza danymi osobowymi powierzanymi na podstawie zawartej umowy głównej. Każdorazowa zmiana zakresu powierzonych do przetwarzania danych wymaga pisemnego aneksu.

## §3
## Obowiązki Podmiotu przetwarzającego i Administratora

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych. Podmiot przetwarzający nie jest uprawniony do korzystania z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej pisemnej zgody Administratora. Zgoda, o której mowa w zdaniu pierwszym może wyrażona jedynie przez osoby upoważnione do reprezentacji Administratora, ujawnione w Krajowym Rejestrze Sądowym, bądź pełnomocnika należycie umocowanego przez osoby uprawnione do reprezentowania Administratora.

3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora. Podmiot przetwarzający nie może przekazywać powierzonych mu danych osobowych osobom trzecim ani do państw trzecich.

4. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

5. Podmiot przetwarzający zobligowany jest zapewnić by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania w tajemnicy przetwarzanych danych zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym bez względu na podstawę prawną zatrudnienia, jak i po jego ustaniu.

6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Administratora trwale usuwa bądź zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi, poprzez odpowiednie środki techniczne i administracyjne, w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

8. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z realizacją obowiązku, o którym mowa w zdaniu poprzedzającym, Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi, nie później jednak niż w ciągu 12 godzin od stwierdzenia naruszenia.

## §4
## Prawo kontroli

1) Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2) Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum trzydniowym uprzedzeniem. O realizacji prawa kontroli Administrator informuje Podmiot przetwarzający pisemnie, faxem, telefonicznie bądź e-mailowo. Strony wskazują następujące dane do kontaktu:

   2.1. Administrator:

      2.1.1. telefon: 22 511 62 00

      2.1.2. fax: 22 511 63 16 (kancelaria)

      2.1.3. adres e-mailowy: spkso@spkso.waw.pl

   2.2. Podmiot przetwarzający:

      2.2.1. telefon:

      2.2.2. fax:

      2.2.3. adres e-mailowy:

3. Zmiana danych kontaktowych, o których mowa w ust. 2 nie wymaga pisemnego aneksu i następuje przez poinformowanie drugiej Strony na piśmie na adres wskazany w komparycji niniejszej umowy o aktualnych danych kontaktowych. W przypadku zmiany adresu do korespondencji i niepoinformowania o tym drugiej Strony, doręczenie na adres wskazany w umowie będzie skuteczne, na co Strony wyrażają zgodę.

4. W przypadku stwierdzenia przez Administratora, bądź audytora uchybień podczas kontroli, o której mowa w ust. 1, Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 3 dni.
5. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych, przy czym zgoda może być wyrażona jedynie przez osoby upoważnione do reprezentacji Administratora, ujawnione w Krajowym Rejestrze Sądowym, bądź pełnomocnika należycie umocowanego przez osoby uprawnione do reprezentowania Administratora.

2. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie. Podmiot przetwarzający obowiązany jest nałożyć na podwykonawcę na mocy odrębnej umowy - te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym regulującym relacje w zakresie ochrony danych osobowych między Administratorem a Podmiotem przetwarzającym, o których to obowiązkach mowa w § 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny Podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Procesorze.

§ 6
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez prezesa Urzędu Ochrony Danych Osobowych. Poinformowanie winno nastąpić w sposób zapewniający bezpieczeństwo przekazywanych informacji. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych. W zakresie przewidzianym w zdaniach poprzedzających Podmiot przetwarzający wdroży wszelkie środki koniecznie do zapobieżenia bądź usunięcia negatywnych skutków prawnych oraz ewentualnych szkód. W szczególności Podmiot przetwarzający zobowiązany jest podjąć wszelkie dozwolone prawnie działania, mające na celu usunięcie skutków naruszeń i zabezpieczenie danych osobowych przed dalszymi naruszeniami, mając na uwadze interes osób, których dane są przetwarzane oraz Administratora.

3. Za działania bądź zaniechania osób, którym Procesor powierza wykonywanie zobowiązań wynikających z niniejszej Umowy, lub z pomocą których takie zobowiązania wykonuje, Procesor odpowiada wobec Administratora jak za działania własne. Procesor nie może czynić jakichkolwiek potrąceń w przypadku posiadania wobec Administratora roszczeń z innych umów, z roszczeniami Administratora wobec Procesora wynikającymi z naruszeniem postanowień niniejszej Umowy. Odpowiedzialność Procesora ma charakter gwarancyjny.

4. W przypadku, gdy za niezgodne z przepisami prawa ( w szczególności Rozporządzenia) bądź postanowieniami niniejszej Umowy działania lub zaniechania Podmiotu przetwarzającego, podwykonawców bądź osób, o których mowa w ust. 3, Administratorowi zostanie wyrządzona szkoda, Podmiot przetwarzający obowiązany jest do jej naprawienia w pełnej wysokości. W szczególności dotyczy to obowiązku zwrotu na rzecz Administratora wszelkich poniesionych przez Administratora kosztów (w szczególności odszkodowań, zadośćuczynień, kosztów sądowych, kar administracyjnych), bez osobnego wezwania ze strony Administratora.

5. W przypadku wytoczenia przeciwko Administratorowi jakiegokolwiek postępowania sądowego (w szczególności cywilnego bądź karnego) lub postępowania administracyjnego, związanego z niezgodnym przetwarzaniem przez Procesora bądź jego podwykonawców lub innych osób bądź podmiotów, z którymi współpracuje powierzonych danych osobowych, Procesor zobowiązany jest do pełnego współdziałania z Administratorem w toku takich postępowań, a jeżeli będzie to możliwe do niezwłocznego wstąpienia do postępowania w miejsce Administratora i zwolnienie Administratora z wszelkich zobowiązań.

## §7
## Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia ..... r. przez cały okres trwania Umowy głównej.
2. Każda ze stron może rozwiązać niniejszą umowę z zachowaniem miesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego. W przypadku rozwiązania umowy, Podmiot przetwarzający obowiązany jest do usunięcia bądź zwrotu (wedle wyboru Administratora) posiadanych przez niego danych osobowych. Usunięcie bądź zwrot nastąpi w terminie siedmiu dni od zgłoszenia takiego żądania przez Administratora nie później jednak niż do dnia rozwiązania niniejszej Umowy. Obowiązek określony w zdaniu poprzedzającym stosuje się odpowiednio do podwykonawców Procesora.

## §8
## Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
   2) przetwarza dane osobowe w sposób niezgodny z przepisami prawa, w szczególności postanowieniami Rozporządzenia bądź z Umową,
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

2. W przypadku rozwiązania umowy w trybie o którym mowa w ust. 1 Podmiot przetwarzający obowiązany jest do usunięcia bądź zwrotu (wedle wyboru Administratora) posiadanych przez niego danych osobowych. Usunięcie bądź zwrot nastąpi niezwłocznie nie później niż w terminie siedmiu dni od dnia rozwiązania umowy.

## §9
## Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne"). Obowiązek określony w zdaniu poprzedzającym stosuje się odpowiednio do podwykonawców Procesora, oraz wszelkich osób lub podmiotów z pomocą których Procesor przetwarza powierzone przez Administratora dane osobowe.

2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez

pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy. Zgoda, o której mowa w zdaniu pierwszym może wyrażona jedynie przez osoby upoważnione do reprezentacji Administratora, ujawnione w Krajowym Rejestrze Sądowym, bądź pełnomocnika należycie umocowanego przez osoby uprawnione do reprezentowania Administratora.

## §10
## Postanowienia końcowe

1. Załączniki stanowią integralną część Umowy.
2. Podmiot przetwarzający nie może przenosić praw i obowiązków wynikających z niniejszej Umowy na podmioty trzecie bez zgody Administratora wyrażonej na piśmie. Zgoda, o której mowa w zdaniu poprzedzającym może wyrażona jedynie przez osoby upoważnione do reprezentacji Administratora, ujawnione w Krajowym Rejestrze Sądowym, bądź pełnomocnika należycie umocowanego przez osoby uprawnione do reprezentowania Administratora.
3. W sprawach nieuregulowanych zastosowanie będą miały zastosowanie przepisy Rozporządzenia, Kodeksu cywilnego oraz inne powszechnie obowiązujące przepisy prawa.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator danych Podmiot przetwarzający