Fundusze Europejskie infrastruktura i środowisko | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Kamień Pomorski dnia 16.10.2023 r.

ZAPYTANIE OFERTOWE NR 1/2023/UE

Powiatowa Stacja Sanitarno-Epidemiologiczna w Kamieniu Pomorskim, zwraca się z zapytaniem o ofertę cenową na n/w towar:

L.p.	OPIS PRZEDMIOTU ZAMÓWIENIA		
	Nazwa oraz szczegółowy opis przedmiotu zamówienia	**Ilość**	**Termin ważności / gwarancji**
1	**System bezpieczeństwa (UTM) z 5 letnią subskrypcją:** - **minimalne wymagania/ specyfikacja techniczna zgodnie z załącznikiem do zapytania ofertowego.** - sprzęt fabrycznie nowy; - karta gwarancyjna; - instrukcja obsługi i dokumentacja techniczna oferowanego sprzętu; - dokumenty określające zasady świadczenia usług przez autoryzowany serwis w okresie gwarancyjnym i pogwarancyjnym; - licencja jak również wszelkie prawa na dostarczone programy i systemy operacyjne, wystawione na rzecz Zamawiającego; - odbiór w siedzibie PSSE zakończony protokołem zdawczo-odbiorczym; - wzór umowy stanowi załącznik do zapytania ofertowego.	szt. 2	60 m-cy

- **Wraz z ofertą należy przedłożyć uzupełniony załącznik do zapytania ofertowego określający model oferowanego urządzenia oraz jego parametry.**
- ***Termin realizacji zamówienia: w terminie do 14 dni od dnia zawarcia umowy, maksymalny czas dostawy 30 listopada 2023 r.***
- ***Odpowiedź do dnia: 20.10.2023 r. godz. 13:00***
- ***Ważność oferty: 30 dni***
- ***Forma płatności: Faktura z odroczonym terminem płatności (przelew 30 dni)***

Dane do faktury:
Powiatowa Stacja Sanitarno – Epidemiologiczna w Kamieniu Pomorskim
ul. Wolińska 7b, 72-400 Kamień Pomorski
NIP: 986-00-08-000

SPECJALISTA
mgr Monika Dementow

TECHNIK INFORMATYK
Tomasz Wieczorek

Osoba kontaktowa:
Monika Dementow, Tomasz Wieczorek
tel. (91) 38 20 144 wew. 244
e-mail: kadry.psse.kamienpomorski@sanepid.gov.pl

DYREKTOR
Powiatowej Stacji Sanitarno-Epidemiologicznej
w Kamieniu Pomorskim
mgr Anna Banasiak

Wymagania ogólne

W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta.

System bezpieczeństwa (UTM) - 2 sztuki

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie usług dostarczanych od dostawcy łącza internetowego.

Wymagania minimalne	**Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.)**
Należy podać producenta i oferowany model	
System realizujący funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.	
System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	
System musi wspierać protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji,. • Protokołów routingu dynamicznego	
Redundancja, monitoring i wykrywanie awarii	
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewnić funkcję synchronizacji sesji.	
System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
System musi umożliwić monitoring stanu realizowanych połączeń VPN.	
System musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	
Interfejsy, Dysk, Zasilanie	
System musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portów Gigabit Ethernet RJ-45.	
System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie	

modemu 4G/5G oraz instalacji oprogramowania z klucza USB.	
System realizujący funkcję firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności 128 GB.	
System musi umożliwić skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.	
System musi być wyposażony w zasilanie AC wraz z zasilaczem.	
Parametry wydajnościowe	
W zakresie Firewall'a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę	
Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.	
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.	
Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.	
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix-1.4 Gbps.	
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - 700 Mbps.	
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - 600 Mbps.	
Funkcje Systemu Bezpieczeństwa	
W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje:	
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	
Kontrola Aplikacji.	
Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	
Ochrona przed malware.	
Ochrona przed atakami - Intrusion Prevention System.	
Kontrola dostępu do stron WWW.	
Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.	
Zarządzanie pasmem (QoS, Traffic shaping).	
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	
Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla	

tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN.	
Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.	
Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	
Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	
Polityki, Firewall	
W ramach polityk i firewalla muszą być realizowane wszystkie poniższe funkcje:	
Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	
System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	
W ramach systemu możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	
System wykorzystuje w politykach bezpieczeństwa zewnętrzne repozytoria zawierających: kategorie URL, adresy IP.	
Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.	
System posiada możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.	

Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	
Połączenia VPN	
W ramach połączeń VPN muszą być realizowane wszystkie poniższe funkcje:	
System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewnić: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to- Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to- Site.	
System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewnić: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.	

• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	
Routing i obsługa łączy WAN	
W zakresie routingu rozwiązanie musi zapewnić obsługę:	
Routingu statycznego.	
Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).	
Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.	
Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.	
ECMP (Equal cost multi-path) - wybór wielu równoważnych tras w tablicy routingu.	
BFD (Bidirectional Forwarding Detection).	
Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	
Funkcje SD-WAN	
System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	
SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	
Zarządzanie pasmem	
System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	
System daje możliwość określania pasma dla poszczególnych aplikacji.	
System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	
System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.	
Ochrona przed malware	
W ramach systemu ochrony przez malware muszą być realizowane wszystkie poniższe funkcje:	
Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	
Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.	
System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów	

zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.	
System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.	
System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego).	
Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandboxw chmurze.	
System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	
Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	
Ochrona przed atakami	
W ramach systemu ochrony przed atakami muszą być realizowane wszystkie poniższe funkcje:	
Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	
System chroni przed atakami na aplikacje pracujące na niestandardowych portach.	
Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.	
System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	
System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.	
Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).	
Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.	
Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	

Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	
Kontrola aplikacji	
W ramach kontroli aplikacji muszą być realizowane wszystkie poniższe funkcje:	
Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	
Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	
Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	
Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.	
Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).	
System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	
Kontrola WWW	
W ramach kontroli *WWW* muszą być realizowane wszystkie poniższe funkcje:	
Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	
W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamie DNS, proxy.	
Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.	
Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.	
Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).	
Filtr WWW daje możliwość wykonania akcji typu „Warning" - ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.	
Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.	

Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.	
System pozwala określić, dla których kategorii URL lub] wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	
Uwierzytelnianie użytkowników w ramach sesji	
W ramach uwierzytelnianie użytkowników w ramach sesji muszą być realizowane poniższe funkcje:	
System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	
System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.	
System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.	
Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	
Zarządzanie	
W ramach systemu zarządzania muszą być realizowane wszystkie poniższe funkcje:	
Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.	
Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.	
Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	
System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz 1 umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.	
System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia ! dokumentację.	
Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	

Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).	
Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	
Logowanie	
W ramach systemu logowania muszą być realizowane wszystkie poniższe funkcje:	
Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.	
W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	
Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.	
Możliwość włączenia / wyłączenia logowania per reguła w polityce firewall.	
System zapewnia możliwość logowania do serwera SYSLOG.	
Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS,	
Testy wydajnościowe oraz funkcjonalne	
Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy wydajnościowe.	
Serwisy i licencje	
Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.	
Gwarancja oraz wsparcie	
Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware	

replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	
Rozszerzone wsparcie serwisowe AHB/SOS	
System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres co najmniej 60 miesięcy.	
Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie. dłuższy niż 1 godzina - reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.	
Wymagania powinny być potwierdzone dokumentami: • Oświadczanie wykonawcy lub producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) dołączyć do oferty. • Certyfikat ISO 9001 lub równoważny podmiotu serwisującego należy załączyć do oferty.	
Technologia podwójnego zastosowania	
W przypadku zaistnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania Wykonawca składa niezbędne oświadczenie.	
Należy dołączyć do oferty dokument - oświadczenie wykonawcy lub producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferowane produkty pochodzą z autoryzowanego kanału sprzedaży.	

TECHNIK INFORMATYK
Tomasz Wieczorek

SPECJALISTA
mgr Monika Dementow

DYREKTOR
Powiatowej Stacji Sanitarno-Epidemiologicznej
w Kamieniu Pomorskim
mgr Anna Banasiak
specjalista ds. epidemiolog

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

UMOWA Nr.....

zawarta w dniu .....2023 r. w..... pomiędzy:
Skarbem Państwa -..... w ....., . ul....., ...,
NIP....., REGON: .....,
zwanym w dalszej treści niniejszej umowy „Zamawiającym",
którego reprezentuje:

1) .....
2) .....

a

....., NIP....., REGON ....., KRS.....
zwanym w dalszej części umowy, „Wykonawcą"
którego reprezentuje:

- .....

§1

Niniejsza umowa zostaje zawarta w wyniku dokonania przez Zamawiającego wyboru oferty Wykonawcy, na podstawie rozeznania rynku na zakup systemu bezpieczeństwa (UTM) z 5 letnią subskrypcją z wyłączeniem stosowania przepisów art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

§2

1. Przedmiotem zamówienia jest dostawa .....
2. Szczegółowy opis przedmiotu zamówienia (OPZ) zawarty jest w załączniku nr 1 do umowy.
3. Wykonawca oświadcza, że przedmiot umowy określony w ust. 1 spełnia wymagania określone w OPZ i jest zgodny z ofertą Wykonawcy stanowiącą integralną część Umowy.
4. Wykonawca oświadcza, że przedmiot umowy jest fabrycznie nowy, nie poleasingowy, nieużywany oraz nieeksponowany na wystawach, pochodzi z autoryzowanego źródła sprzedaży, sprawny technicznie, wolny od wad prawnych i fizycznych, bezpieczny, kompletny i gotowy do pracy, a także spełnia wymagania techniczno-funkcjonalne wyszczególnione w szczegółowym OPZ.
5. Zamawiający i Wykonawca wybrany w postępowaniu o udzielenie zamówienia zobowiązani są współdziałać przy wykonaniu umowy w sprawie zamówienia publicznego, w celu należytej realizacji zamówienia.
6. Wykonawca oświadcza, że przedmiot umowy określony w ust. 1 jest dopuszczony do obrotu prawnego na terytorium RP.
7. Asortyment składający się na przedmiot zamówienia musi spełniać wszelkie wymogi norm określonych obowiązującym prawem.
8. Przed podpisaniem protokołu odbioru Wykonawca przekaże Zamawiającemu komplet dokumentów w języku polskim/ angielskim, w szczególności:
    1) karty gwarancyjne,
    2) instrukcje obsługi i dokumentację techniczną oferowanego sprzętu,
    3) dokumenty określające zasady świadczenia usług przez autoryzowany serwis w okresie gwarancyjnym i pogwarancyjnym,

4) licencje jak również wszelkie prawa na dostarczone programy i systemy operacyjne, wystawione na rzecz Zamawiającego.

9. Przedmiot zamówienia jest współfinansowany na podstawie wspólnej realizacji projektu „Wzmocnienie infrastruktury powiatowych stacji sanitarno-epidemiologicznych w celu zwiększenia efektywności ich działania" realizowanego w ramach osi priorytetowej XI REACT-EU działania 11.3 Wspieranie naprawy i odporności systemu ochrony zdrowia Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020 w zakresie wsparcia organów Państwowej Inspekcji Sanitarnej, opartego na porozumieniu zawartym pomiędzy Głównym Inspektoratem Sanitarnym a każdą z Powiatowych Stacji Sanitarno- Epidemiologicznych będących Zamawiającym.

§3

1. Wykonawca zobowiązuje się zrealizować przedmiot umowy na podstawie niniejszej umowy.
2. Termin dostawy przedmiotu umowy - **do 14 dni od dnia zawarcia umowy.**
3. Jeżeli zwłoka, w stosunku do terminu określonego w ust. 2, przekroczy 3 dni robocze, Zamawiający zastrzega sobie prawo odstąpienia od Umowy z winy Wykonawcy.
4. Przedmiot umowy Wykonawca dostarczy na własny koszt i ryzyko do .....
5. Transport przedmiotu zamówienia krajowy i zagraniczny wraz z ubezpieczeniem, wszelkimi opłatami celnymi, skarbowymi oraz innymi opłatami pośrednimi obciążają Wykonawcę.
6. Wykonawca zobowiązuje się co najmniej na 3 dni przed planowanym terminem dostawy, powiadomić Zamawiającego drogą elektroniczną na adres poczty elektronicznej: .... o dacie i godzinie dostawy.
7. Odbiór będzie polegał na stwierdzeniu zgodności z OPZ oraz Ofertą Wykonawcy, w szczególności braku uszkodzeń mechanicznych, pochodzenia z autoryzowanego źródła czy poprawności działania. Z czynności odbioru zostanie sporządzony protokół odbioru Przedmiotu Umowy. Protokół winien dodatkowo zawierać wszelkie uwagi i zastrzeżenia w tym w zakresie pochodzenia przedmiotu umowy z autoryzowanego źródła.
8. W przypadku stwierdzenia wad lub niezgodności Przedmiotu Umowy z treścią OPZ lub Ofertą Wykonawcy lub postanowieniami niniejszej umowy, w szczególności stwierdzenia uszkodzeń mechanicznych, niezgodności w zakresie parametrów technicznych jak i funkcjonalnych, pochodzenia przedmiotu umowy z nie autoryzowanego źródła Wykonawca niezwłocznie, ale nie później niż w terminie 7 dni, dokona wymiany przedmiotu umowy na wolny od stwierdzonych wad lub niezgodności z treścią z OPZ. Nie dokonanie wymiany, w powyższym terminie, skutkuje uprawnieniem Zamawiającego do odstąpienia od umowy z winy Wykonawcy.
9. Do koordynacji spraw związanych z przedmiotem zamówienia Wykonawca upoważnia .....tel. ....., e-mail:.....
10. Do koordynacji spraw związanych z przedmiotem zamówienia Zamawiający upoważnia.... ..... tel. .....e-mail: .....

§4

1. Za prawidłowe wykonanie Przedmiotu umowy, Zamawiający zapłaci Wykonawcy **cenę brutto.....złotych** (słownie): ....., w tym podatek VAT 23%.
2. Wynagrodzenie Wykonawcy obejmuje wszystkie elementy przedmiotu zamówienia wymienione w OPZ.
3. Rozliczenie nastąpi w formie przelewu z konta Zamawiającego na konto Wykonawcy w terminie do 30 dni kalendarzowych, licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury. Termin, o którym mowa w zdaniu pierwszym jest zastrzeżony na korzyść Zamawiającego. Podanie na fakturze terminu płatności innego niż w zdaniu powyżej nie zmienia warunków płatności.
4. Podstawą wystawienia faktury przez Wykonawcę jest podpisany przez Zamawiającego bez zastrzeżeń protokół odbioru, o którym mowa w § 3 ust. 7 Umowy.
5. Za datę dokonania przez Zamawiającego płatności uznaje się datę złożenia przelewu należności w banku Zamawiającego.
6. Jeśli numer rachunku rozliczeniowego wskazany przez Wykonawcę jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - *Prawo Bankowe* prowadzony jest rachunek VAT to:
   1) Zamawiający oświadcza, że będzie realizować płatności za faktury z zastosowaniem mechanizmu podzielonej płatności tzw. „split payment". Zapłatę w tym systemie uznaje się za dokonanie płatności w terminie ustalonym w ust. 3,
   2) Podzieloną płatność tzw. „split payment" stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata kar, odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0% lub objęte odwrotnym obciążeniem,
   3) Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności tzw. „split payment".

§5

1. Na przedmiot umowy Wykonawca udziela **60 miesięcznej gwarancji.**
2. Okres rękojmi jest tożsamy z okresem gwarancji.
3. Termin udzielonej gwarancji i rękojmi rozpoczyna bieg od momentu aktywacji licencji na urządzeniu, o którym mowa w § 2 ust. 1.
4. Wykonawca, w okresie gwarancji, gwarantuje czas reakcji serwisu zgodnie z wymaganiami określonymi w OPZ.
5. Okres trwania gwarancji i rękojmi będzie automatycznie wydłużony od dnia zgłoszenia

wady lub nieprawidłowości działania urządzenia do czasu faktycznego jego naprawienia i udostępnienia go Zamawiającemu.

6. Wszelkie koszty związane ze świadczeniem usług gwarancyjnych obciążają Wykonawcę.
7. W razie nieuwzględnienia reklamacji przez Wykonawcę, Zamawiający może wystąpić z wnioskiem o przeprowadzenie ekspertyzy przez rzeczoznawcę z danej dziedziny.
8. Jeżeli reklamacja Zamawiającego okaże się uzasadniona, koszty związane z przeprowadzeniem ekspertyzy oraz koszty związane z usunięciem wad ponosi Wykonawca.
9. Jeżeli w okresie gwarancji, na skutek dostarczenia przez Wykonawcę wadliwego przedmiotu umowy Zamawiający poniesie dodatkowe koszty związane z wykonywaną w oparciu o wadliwy przedmiot umowy działalnością, Wykonawca zobowiązuje się do zwrotu Zamawiającemu tych kosztów, po uprzednim uzgodnieniu formy zwrotu.
10. Zamawiający ma prawo dochodzić uprawnień przysługujących z tytułu rękojmi za wady, niezależnie od uprawnień wynikających z gwarancji.
11. W przypadku stwierdzenia usterki/wady przedmiotu umowy w okresie objętym gwarancją, Strony komunikują się za pośrednictwem poczty elektronicznej. Korespondencję w powyższym zakresie kierować należy na adres mailowy:
    1) Zamawiającego - .....
    2) Wykonawcy- .....
12. Wykonawca zapewni autoryzowany polskojęzyczny serwis gwarancyjny.

§6

1. Zamawiający ma prawo naliczyć Wykonawcy karę umowną w następujących okolicznościach:
    1) w przypadku odstąpienia od umowy przez Wykonawcę lub Zamawiającego, z przyczyn zawinionych po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wartości wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;
    2) w przypadku zwłoki w realizacji przedmiotu umowy, w terminie określonym w § 3 ust. 2 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1 % wartości wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy za każdy dzień zwłoki;
    3) w przypadku zwłoki w wymianie sprzętu na wolny od wad/na wolny od niezgodności lub naprawie wadliwego przedmiotu umowy, w terminie określonym w § 3 ust. 8 lub § 5 ust. 4 umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5 % wartości wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy za każdy

dzień zwłoki.

2. Limit kar umownych z tytułów przewidzianych w niniejszej umowie wynosi 25 % wartości wynagrodzenia brutto określonego w § 4 ust. 1.
3. Kary umowne stają się wymagalne w pierwszym dniu kiedy możliwe jest ich naliczenie, a w przypadku kar za zwłokę z każdym dniem zwłoki.
4. Zamawiający może dochodzić odszkodowania uzupełniającego przenoszącego wysokość kar umownych na zasadach ogólnych kodeksu cywilnego.
5. Zamawiającemu przysługuje prawo potrącenia kar umownych z wynagrodzenia Wykonawcy. Wysokość oraz rodzaj nałożonej kary zostaną określone przez Zamawiającego w nocie obciążeniowej, którą otrzyma Wykonawca.

§7

1. Zamawiającemu przysługuje w szczególności prawo odstąpienia od umowy w następujących sytuacjach:
   1) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy w całości lub w jej części nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W takiej sytuacji Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy,
   2) dostawy innego przedmiotu umowy niż określony w opisie przedmiotu zamówienia,
   3) jeżeli Wykonawca w chwili złożenia oferty podlegał wykluczeniu na podstawie okoliczności, o których mowa w art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego i złożył w tym zakresie nieprawdziwe oświadczenie,
   4) nie dokonanie wymiany dostarczonego sprzętu, zgodnie z wymogiem zawartym w § 3 ust. 8 umowy,
   5) nie zapewnienie polskojęzycznego serwisu gwarancyjnego.
2. Zamawiający będzie mógł odstąpić od umowy w każdym momencie, od powzięcia wiadomości o okolicznościach stanowiących podstawę odstąpienia.
3. Odstąpienie od niniejszej umowy uznaje się za skuteczne z chwilą doręczenia Wykonawcy oświadczenia Zamawiającego drogą mailową na adres ..... jeśli zostanie potwierdzone następnie listem poleconym wysłanym na adres Wykonawcy.
4. Każda ze Stron może wypowiedzieć lub odstąpić od Umowy w razie zaistnienia przypadku siły wyższej, którego skutkiem jest niemożność wykonania obowiązków wynikających z Umowy przez którąkolwiek ze Stron przez okres ponad 30 dni. Po upływie wskazanego

terminu każda ze Stron może wypowiedzieć lub odstąpić od Umowy ze skutkiem natychmiastowym i w drodze pisemnego oświadczenia przesłanego drugiej Stronie wraz z udowodnieniem tych okoliczności poprzez przedstawienie dokumentacji potwierdzającej wystąpienie zdarzeń mających cechy Siły wyższej oraz wskazania wpływu, jaki zdarzenie miało na przebieg realizacji umowy.

5. Przez pojęcie siły wyższej należy rozumieć zdarzenie zewnętrzne, którego nie można było przewidzieć, analizując i uwzględniając wszystkie okoliczności sprawy, jak również, któremu nie można było zapobiec znanymi, normalnie stosowanymi sposobami w szczególności zdarzenia o charakterze katastrofalnych działań przyrody albo nadzwyczajnych i zewnętrznych wydarzeń, którym zapobiec nie można, jak wojna, konflikt zbrojny na terenach graniczących z Rzecząpospolitą Polską, restrykcje stanu wojennego, powstanie, rewolucja, zamieszki.

§8

1. Przewiduje się możliwości zmiany umowy, gdy:
   1) ulegnie zmianie stan prawny w zakresie dotyczącym realizowanej umowy, który spowoduje konieczność zmiany sposobu wykonania zamówienia przez Wykonawcę;
   2) wystąpią przeszkody o obiektywnym charakterze (zdarzenia nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia, a więc mieszczące się w zakresie pojęciowym tzw. „siły wyższej" w tym klęski żywiołowej). W takim przypadku termin realizacji przedmiotu umowy może ulec przesunięciu o czas trwania przeszkody. Strony zobowiązują się do natychmiastowego poinformowania się nawzajem o wystąpieniu ww. przeszkód;
2. Żadnej ze stron Umowy nie przysługuje roszczenie o zawarcie aneksu (obie strony muszą wyrazić zgodę na zawarcie aneksu).

§9

1. Wykonawca nie ma prawa przenoszenia praw lub obowiązków wynikających z niniejszej umowy na rzecz osób trzecich bez zgody Zamawiającego wyrażonej pod rygorem nieważności na piśmie.
2. Nieważność lub nieskuteczność któregokolwiek z postanowień Umowy nie wpływa na ważność i skuteczność pozostałych jej postanowień. Strony będą dążyły do zastąpienia nieważnego lub nieskutecznego postanowienia przez ważne i skuteczne postanowienie, które pozwoli osiągnąć w sposób jak najbardziej zbliżony taki sam lub podobny cel Umowy.
3. Ewentualne spory wynikłe z niniejszej Umowy rozstrzygane będą przez miejscowo

właściwy Sąd dla siedziby Zamawiającego.

4. Wszelka korespondencja kierowana będzie przez strony wzajemnie na adresy wskazane w nagłówku umowy. Każda ze stron zobowiązana jest niezwłocznie powiadomić drugą stronę o zmianie adresu do doręczeń wskazanego w nagłówku umowy lub pozostałych danych kontaktowych, pod rygorem uznania za prawidłowe doręczenia na dotychczasowy adres.
5. Strony zobowiązują się do wzajemnego, niezwłocznego informowania o każdej zmianie statusu prawnego i adresu siedziby. W przypadku niedopełnienia ww. obowiązków przez którąkolwiek ze Stron, Stronę tę obciążać będą ewentualne koszty mogące wyniknąć wskutek zaniechania.
6. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego.
7. Umowa została sporządzona w formie elektronicznej zgodnie z art. 78^1 § 1 Kodeksu cywilnego pod rygorem nieważności i zawarta w dacie złożenia podpisu przez ostatnią ze Stron.

.....	.....
Zamawiający	**Wykonawca**

Sprawdzono pod względem formalno-prawnym
Radca Prawny dr Sławomir Tomczyk
Kamień Pomorski, dn. 16.10.2023 r.

Załącznik nr 9 do Porozumienia w sprawie wspólnej realizacji Projektu

Wzór klauzuli informacyjnej, stanowiącej realizację obowiązku informacyjnego

Administratorem przetwarzanych danych osobowych jest minister właściwy ds. rozwoju regionalnego, pełniący funkcję Instytucji Zarządzającej Programem Operacyjnym Infrastruktura i Środowisko 2014-2020 (PO IiŚ 2014-2020), z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa.

Minister Zdrowia pełniący funkcję Instytucji Pośredniczącej PO IiŚ 2014-2020 jest podmiotem przetwarzającym dane osobowe na podstawie porozumienia zawartego z administratorem (tzw. procesorem).

Dane osobowe przetwarzane będą na potrzeby realizacji PO IiŚ 2014-2020, w tym w szczególności w celu realizacji projektu w ramach Osi Priorytetowej XI REACT-UE.

Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu, związanego z wdrażaniem Programu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Przetwarzanie danych osobowych odbywa się w związku[1]:

1. z realizacją ciążącego na administratorze obowiązku prawnego (art. 6 ust. 1 lit. c RODO[2]), wynikającego z następujących przepisów prawa[3]:

   - rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006,

   - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/2221 z dnia 23 grudnia 2020 r. zmieniającym rozporządzenie (UE) nr 1303/2013 w odniesieniu do zasobów dodatkowych i przepisów wykonawczych w celu zapewnienia pomocy na wspieranie kryzysowych działań naprawczych w kontekście pandemii COVID-19 i jej skutków społecznych oraz przygotowanie do ekologicznej i cyfrowej odbudowy gospodarki zwiększającej jej odporność (REACT-EU);

   - rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących

[1] Należy wybrać jedną lub kilka podstaw.

[2] 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 (Dz. Urz. UE. L 119 z 04.05.2016, s.1-88).

[3] Należy wskazać jeden lub kilka przepisów prawa - możliwe jest ich przywołanie w zakresie ograniczonym na potrzeby konkretnej klauzuli.

do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi,

- Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012,
- ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020,
- ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego,
- ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,

2. z wykonywaniem przez administratora zadań realizowanych w interesie publicznym lub ze sprawowaniem władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO),
3. z realizacją umowy, gdy osoba, której dane dotyczą, jest jej stroną, a przetwarzanie danych osobowych jest niezbędne do jej zawarcia oraz wykonania (art. 6 ust. 1 lit. b RODO).

Minister może przetwarzać różne rodzaje danych[4], w tym przede wszystkim:

1) dane identyfikacyjne, w tym w szczególności: imię, nazwisko, miejsce zatrudnienia / formę prowadzenia działalności gospodarczej, stanowisko; w niektórych przypadkach także PESEL, NIP, REGON,
2) dane dotyczące zatrudnienia, w tym w szczególności: otrzymywane wynagrodzenie oraz wymiar czasu pracy,
3) dane kontaktowe, w tym w szczególności: adres e-mail, nr telefonu, nr fax, adres do korespondencji,
4) dane o charakterze finansowym, w tym szczególności: nr rachunku bankowego, kwotę przyznanych środków, informacje dotyczące nieruchomości (nr działki, nr księgi wieczystej, nr przyłącza gazowego),

Dane pozyskiwane są bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację Programu, w tym w szczególności: od wnioskodawców, beneficjentów, partnerów.

Odbiorcami danych osobowych mogą być:

- podmioty, którym Instytucja Zarządzająca PO IiŚ 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności podmioty pełniące funkcje Instytucji Pośredniczących i Wdrażających,
- instytucje, organy i agencje Unii Europejskiej (UE), a także inne podmioty, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem PO IiŚ 2014-2020,

[4] Informacje podawane w przypadku wykonywania obowiązku informacyjnego na podstawie art. 14 RODO.

- podmioty świadczące usługi, w tym związane z obsługą i rozwojem systemów teleinformatycznych oraz zapewnieniem łączności, w szczególności dostawcy rozwiązań IT i operatorzy telekomunikacyjni [5].

Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach PO liŚ 2014-2020 - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Osobie, której dane dotyczą, przysługuje:

- prawo dostępu do swoich danych oraz otrzymania ich kopii (art. 15 RODO),
- prawo do sprostowania swoich danych (art. 16 RODO),
- prawo do usunięcia swoich danych (art. 17 RODO) - jeśli nie zaistniały okoliczności, o których mowa w art. 17 ust. 3 RODO,
- prawo do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
- prawo do przenoszenia swoich danych (art. 20 RODO) - jeśli przetwarzanie odbywa się na podstawie umowy: w celu jej zawarcia lub realizacji (w myśl art. 6 ust. 1 lit. b RODO), oraz w sposób zautomatyzowany [6],
- prawo wniesienia sprzeciwu wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO),
- prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych (art. 77 RODO) - w przypadku, gdy osoba uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO lub inne krajowe przepisy regulujące kwestię ochrony danych osobowych, obowiązujące w Rzeczpospolitej Polskiej.

W przypadku pytań, kontakt z Inspektorem Ochrony Danych Osobowych Ministerstwa Funduszy i Polityki Regionalnej i jest możliwy:

- pod adresem: ul. Wspólna 2/4, 00-926 Warszawa,
- pod adresem e-mail: *IOD@mfipr.gov.pl*.

Dane osobowe nie będą objęte procesem zautomatyzowanego podejmowania decyzji, w tym profilowania.

[5] O ile dotyczy.

[6] Do automatyzacji procesu przetwarzania danych osobowych wystarczy, że dane te są zapisane na dysku komputera.