

1. Opis przedmiotu zamówienia:

1.1. W systemie alarmowym Opolskiego Oddziału Regionalnego ARiMR funkcjonuje pięć central alarmowych, a w podległych lokalizacjach zainstalowane jest po jednej centrali alarmowej. Ilość linii dozorowanych nie przekracza 38 dla każdego z obiektów Biur Powiatowych i 150 linii łącznie dla wszystkich stref Oddziału Regionalnego Agencji. Nie jest prowadzony monitoring wizyjny przy wykorzystaniu systemów alarmowych będących przedmiotem postępowania.

1.2. Wymagania techniczne, jakie spełnia aktualnie system alarmowy zainstalowany u Zamawiającego:

- 1.2.1. samoczynne dozorowanie linii wejściowych,*
- 1.2.2. precyzyjne lokalizowanie miejsca powstania alarmu,*
- 1.2.3. możliwość oceny stanu technicznego urządzeń,*
- 1.2.4. zapewnienie dwutorowości monitoringu obiektów (GSM),*
- 1.2.5. obsługa bezprzewodowych przycisków napadowych,*
- 1.2.6. zabezpieczenie antysabotażowych urządzeń systemów.*

1.3. Centrale alarmowe w poszczególnych lokalizacjach:

1.3.1. Centrala alarmowa nr 1 w OR obsługuje:

Obiekt ARiMR OR08, 45-486 Opole ul. Wrocławska 170G parter - BWI.

Obiekt ARiMR OR08, 45-486 Opole ul. Wrocławska 170G parter - BWI Kancelaria.

Obiekt ARiMR OR08 45-486 Opole ul. Wrocławska 170G parter - pomieszczenie ochrony,

Obiekt ARiMR OR08 45-486 Opole ul. Wrocławska 170G piętro I — BOR,

Obiekt ARiMR OR08 45-486 Opole ul. Wrocławska 170G piętro II— BKM.

1.3.2. Centrala alarmowa nr 2 w OR obsługuje:

Obiekt ARiMR OR08 45-486 Opole ul. Wrocławska 170C parter - Magazyn.

1.3.3. Centrala alarmowa nr 3 w OR obsługuje:

Obiekt ARiMR OR08 45-486 Opole ul. Wrocławska 170F parter - Archiwum

1.3.4. Obiekt BP 156 Brzeg 49-340 Lewin Brzeski ul. Moniuszki 14,

1.3.5. Obiekt BP 157 Głubczyce 48-100 Głubczyce ul. Powstańców 4,

1.3.6. Obiekt BP 158 Polska Cerekiew 47-260 Polska Cerekiew ul. Rynek 2,

1.3.7. Obiekt BP 159 Kluczbork 46-200 Kluczbork ul. Waryńskiego 7,

1.3.8. Obiekt BP 160 Krapkowice 47-303 Krapkowice ul. Kilińskiego 1,

1.3.9. Obiekt BP 161 Namysłów 46-100 Namysłów ul. Józefa Piłsudskiego 3,

1.3.10. Obiekt BP 162 Nysa 48-303 Nysa ul. Marcinkowskiego 2 - 4,

1.3.11. Obiekt BP 163 Olesno 46-300 Olesno ul. Powstańców Śląskich 14,

- 1.3.12. Obiekt BP 164 Opole 45-323 Opole ul. Zielonogórska 3 IV piętro,**
- 1.3.13. Obiekt BP 165 Prudnik 48-210 Biała ul. Kościuszki 24,**
- 1.3.14. Obiekt BP 166 Strzelce Opolskie 47-100 Strzelce Opolskie ul. I-go Maja 59.**

1.4. Systemy SKD zarządzane są z sieci LAN Zamawiającego.

1.5. Elementy systemu SKD we wszystkich lokalizacjach Zamawiającego stanowią:

- 1.5.1. Centrala systemu kontroli dostępu,**
- 1.5.2. Kontrolery dostępu jednego przejścia,**
- 1.5.3. Zbliżeniowo-klawiaturowy terminal dostępu,**
- 1.5.4. Interfejs komunikacyjny Ethernet TCP/IP.**

Uwaga: w Biurze powiatowym powiatu prudnickiego (48-210 Biała ul. Kościuszki 24) - system SKD w utrzymaniu administratora Budyńku. - Utrzymanie SKD w tym biurze nie jest objęte przedmiotem zamówienia.

1.6. Elementy systemu wewnętrznego monitoringu wizyjnego

- 1.6.1. Obiekt ARiMR OR08, 45-486 Opole ul. Wrocławska 170G – rejestrator + 8 kamer**
- 1.6.2. Obiekt BP 156 Brzeg 49-340 Lewin Brzeski ul. Moniuszki 14, - Rejestrator + 5 kamer**
- 1.6.3. Obiekt BP 157 Głubczyce 48-100 Głubczyce ul. Powstańców 4, - Rejestrator + 2 kamery**
- 1.6.4. Obiekt BP 158 Polska Cerekiew 47-260 Polska Cerekiew ul. Rynek 2, - Rejestrator + 5 kamer**
- 1.6.5. Obiekt BP 159 Kluczbork 46-200 Kluczbork ul. Waryńskiego 7, - Rejestrator + 5 kamer**
- 1.6.6. Obiekt BP 160 Krapkowice 47-303 Krapkowice ul. Kilińskiego 1, - Rejestrator + 2 kamery**
- 1.6.7. Obiekt BP 161 Namysłów 46-100 Namysłów ul. Józefa Piłsudskiego 3, - Rejestrator + 4 kamery**
- 1.6.8. Obiekt BP 162 Nysa 48-303 Nysa ul. Marcinkowskiego 2 - 4, - Rejestrator + 3 kamery**
- 1.6.9. Obiekt BP 163 Olesno 46-300 Olesno ul. Powstańców Śląskich 14, - Rejestrator + 4 kamery**
- 1.6.10. Obiekt BP 164 Opole 45-323 Opole ul. Zielonogórska 3 IV piętro, - Rejestrator + 2 kamery**

1.6.11. Obiekt BP 165 Prudnik 48-210 Biała ul. Kościuszki 24, - Rejestrator + 2 kamery

**1.6.12. Obiekt BP 166 Strzelce Opolskie 47-100 Strzelce Opolskie ul. I-go Maja 59. -
Rejestrator + 3 kamery**

2. Zakres zadań Wykonawcy wyłonionego w niniejszym postępowaniu:

2.1. Zapewnienie monitoringu lokalu z dojazdem załóg interwencyjnych do każdego z obiektów wymienionych w pkt I.2.1.1, Rozdziału I SWZ, w którym system wykrył zagrożenie.

2.1.1. Wykonawca w ramach monitoringu powinien zapewnić:

2.1.1.1. monitorowanie obiektów, o których mowa w pkt I.2.1.1, Rozdziału I SWZ,
za pomocą komunikacji GSM,

2.1.1.2. montaż i włączenie do istniejących systemów Zamawiającemu:

2.1.1.2.1. w okresie obowiązywania umowy Wykonawca będzie zobowiązany do zapewnienia dwóch niezależnych modułów GSM we wszystkich lokalnych systemach alarmowych. Moduły GSM pozostaną własnością Wykonawcy. Koszty eksploatacji w trakcie realizacji zamówienia, w tym realizowanych połączeń, obciążają Wykonawcę;

2.1.1.2.2. zapewnienie dwóch oddzielnych kanałów monitoringu wszystkich obiektów ze względu na brak możliwości instalacji łączy na linii komutowanej Zamawiający przyjmuje rozwiązanie monitoringu oparte na dwóch niezależnych modułach GSM oraz usługi transmisji danych przez dwóch różnych operatorów telekomunikacyjnych;

2.1.1.3. przyjmowanie informacji o zdarzeniach, przesłanych z lokalnych central alarmowych, zainstalowanych w obiektach Zamawiającego do Stacji Monitorowania Alarmów (SMA) Wykonawcy. Informacja przesyłana będzie poprzez komunikację opartą o GSM. Następnie drogą telefoniczną oraz SMS-em przekazanie informacji o zdarzeniach osobom wyznaczonym przez Zamawiającego do powiadamiania w przypadku powstania alarmu, zgodnie z wykazem w załączniku nr 10 do SWZ;

2.1.1.4. telefoniczne sprawdzanie sytuacji w obiekcie po wywołanym alarmie w czasie godzin pracy - dyspozytor Stacji Monitorowania Alarmu (SMA) telefonuje pod wskazany numer, sprawdza przyczynę i okoliczności alarmu;

2.1.1.5. testowanie z wykorzystaniem komunikacji GSM poprawności działania systemów alarmowych z częstotliwością, co 60 sekund oraz niezwłoczne informowanie Zamawiającego o powstałych awariach;

- 2.1.1.6. sprawdzenie poprawności komunikacji;
- 2.1.1.7. utrzymywanie w pełnej sprawności systemu alarmowego, przeciwpożarowego oraz systemu kontroli dostępu i monitoringu wizyjnego w obiekcie;
- 2.1.1.8. kontrolę czasu uzbrojenia i rozbrojenia systemu alarmowego;
- 2.1.1.9. niezwłoczne (automatyczne) przesyłanie informacji sms na wskazane telefony komórkowe pracowników Zamawiającego o alarmie lub usterce systemu alarmowego. Zamawiający przekaże co najmniej dwa numery telefonów komórkowych, które te informacje będą otrzymywać;
- 2.1.1.10. bezzwłoczne powiadomienie Zamawiającego - w drodze telefonicznej, mailem, a następnie pisemnie - o braku możliwości monitorowania lokalnego systemu alarmowego oraz o zaistniałym uszkodzeniu urządzeń przekazu sygnału alarmowego;
- 2.1.1.11. niezwłoczne powiadamianie Zamawiającego o wszelkich zmianach i zdarzeniach, które mogłyby mieć wpływ na prawidłowe wykonanie umowy przez Wykonawcy;
- 2.1.1.12. dostarczenie - na pisemny wniosek Zamawiającego - wydruku stanów pracy lokalnego systemu alarmowego za miniony lub trwający miesiąc oraz wydruków testowania po łączach GSM poprawności działania systemów alarmowych;
- 2.1.1.13. usuwanie wad i uszkodzeń systemu;
- 2.1.1.14. postępowanie zgodnie z instrukcją określoną w załączniku nr 11 do SWZ;
- 2.1.1.15. kontynuacje realizacji świadczenia w okresie ogłoszonego przez organy władzy terenowej lub państwowej stanu klęski żywiołowej, stanu wyjątkowego lub stanu wojny;
- 2.1.1.16. aktualizacje i stworzenie dokumentacji technicznej wszystkich urządzeń i systemów zabezpieczeń zlokalizowanych w obiektach jednostek Opolskiego Oddziału Regionalnego w terminie do 31.01.2024 roku przesyłając drogą elektroniczną na adres osoby uprawnionej do kontaktu ze strony Zamawiającego wskazanej w §15 ust. 7 pkt 2 umowy oraz przekazanie wersji papierowej na adres Zamawiającego nie później niż do 08.02.2024 r.**
- 2.1.1.17. umożliwienie z sieci publicznej Internet podglądu zdarzeń wszystkich monitorowanych obiektów zajmowanych przez Zamawiającego bezpośrednio na stacji monitoringu Wykonawcy przez wliczone w wynagrodzenie z pkt.2.1 dedykowane oprogramowanie dostarczone przez Wykonawcę dla wyznaczonych pracowników Zamawiającego.

2.1.2. Utrzymywanie urządzeń i systemów monitoringu w stanie zapewniającym sprawne funkcjonowanie systemu przez cały okres obowiązywania umowy.

- 2.1.2.1. Wykonawca jest zobowiązany do utrzymywania urządzeń i systemów w stanie zapewniającym sprawne funkcjonowanie systemów (alarmowych / przeciwpożarowych

/ kontroli dostępu / monitoringu wizyjnego we wszystkich obiektach zajmowanych przez Zamawiającego) przez cały okres obowiązywania umowy;

- 2.1.2.2. utrzymanie, w tym czynności i całkowite koszty usuwania ewentualnej awarii systemu tj. uszkodzenie lub zepsucie się elementu(ów) instalacji systemów (alarmowych / przeciwpożarowych / kontroli dostępu/ monitoringu wizyjnego we wszystkich obiektach zajmowanych przez Zamawiającego) powodujące jej całkowitą bądź częściową niesprawność są wliczone na zasadzie ryzyka ryczałtowego Wykonawcy w cenę o której mowa w kolumnie C dla pozycji 1 tabeli nr 1 załącznika nr 2 do SWZ;
- 2.1.2.3. w przypadku wykrycia awarii jakiegokolwiek elementu w systemie, w tym też w SKD/ monitoringu wizyjnego, Zamawiający niezwłocznie po powzięciu takiej informacji zgłosi ją Wykonawcy w formie faxu lub pocztą elektroniczną, przez osoby upoważnione do takiego kontaktu przez Zamawiającego (w godzinach pracy Zamawiającego), bądź w drodze telefonicznej (po godzinach pracy Zamawiającego) wg załącznika nr 14 do SWZ;
- 2.1.2.4. w przypadku wykrycia przez Wykonawcę awarii lub wady systemu, Wykonawca jest zobowiązany do niezwłocznego, w drodze telefonicznej bądź e-mail, zawiadomienia Zamawiającego oraz niezwłocznego przystąpienia do usuwania awarii;
- 2.1.2.5. Wykonawca ma obowiązek po powzięciu informacji o awarii do niezwłocznego przystąpienia do ich usuwania;
- 2.1.2.6. Wykonawca jest obowiązany do zapewnienia całodobowej gotowości serwisowej z zapewnieniem dojazdu do uszkodzonego systemu alarmowego do 3 godziny w Opolu i do 6 godzin w pozostałych miejscowościach licząc od momentu wykrycia awarii bądź od momentu powzięcia informacji o awarii;
- 2.1.2.7. Naprawa zostanie potwierdzona protokołem wg załącznika nr 12 do SWZ podpisanym przez przedstawicieli stron oraz w książce przeglądów i konserwacji / napraw wg załącznika nr 13 do SWZ;
- 2.1.2.8. Wykonawca na czas sprowadzenia nowego elementu zapewni tymczasowy element w miejsce wadliwego o nie gorszych parametrach w celu zapewnienia nieprzerwanego funkcjonowania systemów (alarmowych / przeciwpożarowych / kontroli dostępu/ monitoringu wizyjnego) we wszystkich obiektach zajmowanych przez Zamawiającego;
- 2.1.2.9. Dojazd do miejsca usunięcia awarii wliczony jest w cenę.

2.1.3. Interwencja grupy interwencyjnej

- 2.1.3.1. Wykonawca w ramach realizacji monitoringu zapewni interwencję grupy interwencyjnej polegającą na wysyłaniu załogi interwencyjnej, która bezpośrednio po powiadomieniu przez SMA o alarmie niezwłocznie uda się do zagrożonego obiektu Zamawiającego i podejmie działania zmierzające do ujęcia sprawcy czynu zabronionego prawem,

zabezpieczenia mienia Zamawiającego oraz osób do czasu przyjazdu Zamawiającego lub osób powiadomionych przez Wykonawcę, wraz z niezwłocznym powiadomieniem o zdarzeniu organów Policji i zabezpieczeniem obiektów do czasu jej przybycia, a w razie zagrożenia pożarem powiadomienie także Jednostek Straży Pożarnej. Dojazd załogi interwencyjnej wraz z prowadzoną przez nią pierwszą godziną interwencji doraźnej jest wliczony w cenę świadczenia z pkt.2.1. Zamawiający przewiduje możliwość weryfikacji faktycznego czasu dojazdu grupy interwencyjnej do poszczególnych obiektów, który liczony będzie od momentu przekazania sygnału alarmowego w sposób określony w pkt 2.1.3.2.1.

2.1.3.2. Warunki realizacji:

2.1.3.2.1. interwencje załogi interwencyjnej będą realizowane w wyniku przekazania sygnału alarmowego poprzez użycie radiowego przycisku napadowego, znajdującego się w każdym z obiektów;

2.1.3.2.2. załoga interwencyjna w przypadku stwierdzenia włamania, pożaru lub innych zdarzeń, w których niezbędne jest zabezpieczenie lokalu pozostaje na miejscu zdarzenia zabezpieczając obiekt do momentu odwołania przez uprawnionego pracownika ARiMR;

2.1.3.2.3. maksymalny czas dojazdu załogi interwencyjnej do poszczególnych obiektów liczony od wystąpienia alarmu w danym obiekcie nie dłuższy niż 15 minut, w godzinach 6.00 - 22.00 oraz nie dłuższy niż 10 minut w godzinach 22.00 - 6.00, a w przypadku Biura Powiatowego w Lewinie Brzeskim, w Oleśnie i w Polskiej Cerekwi: nie dłuższy niż 20 minut w godzinach 6.00 - 22.00 oraz nie dłuższy niż 15 minut w godzinach 22.00 - 6.00. Nieterminowy przyjazd Wykonawcy będzie sankcjonowany wszystkimi dostępnymi środkami prawnymi wynikającymi z treści załącznika nr 8 do SWZ (w tym m.in. każdorazowe naliczanie kary umownej) oraz na podstawie prawa powszechnie stanowionego.

2.1.3.3. Interwencja grupy interwencyjnej na alarm monitoringu zawiniony przez czynności pracownika Zamawiającego (tj. brak rozbiorzenia systemu alarmowego przy otwieraniu biura przez pracownika Zamawiającego oraz skutki pozostawienia przez pracownika Zamawiającego otwartego okna w biurach) jest płatna za każdą rozpoczętą godzinę (w tym pierwszą) interwencji doraźnej na miejscu zdarzenia w ramach prawa opcji zakupu o której mowa w pkt.2.6 z zastrzeżeniem pkt. 2.1.3.4. Koszt dojazdu na taką interwencję jest wliczony w cenę pierwszej roboczogodziny interwencji doraźnej o której mowa w pkt.2.6.

2.1.3.4. W przypadku pierwszej w danym miesiącu interwencji doraźnej w każdym chronionym obiekcie Zamawiającego, pierwsza godzina takiej interwencji wraz z dojazdem jest wliczona w wynagrodzenie za monitoring z pkt.2.1. W takim przypadku zastosowanie

wynagrodzenia dla pkt.2.6 jest możliwe dopiero od kolejnej rozpoczętej godziny danej interwencji doraźnej.

2.1.3.5. Wyjazd grupy interwencyjnej na fałszywy alarm niezawiniony przez pracowników Zamawiającego stanowi realizację świadczenia i jest wyłącznym kosztem Wykonawcy stanowiącym jego ryzyko ryczałtowe z wynagrodzenia dla pkt.2.1.

2.2. Świadczenie usługi ochrony fizycznej mienia wraz z dozorem dziennym nieruchomości zabudowanej będącej w eksploatacji Opolskiego Oddziału Regionalnego ARiMR zlokalizowanej przy ul. Wrocławskiej 170 w Opolu:

2.2.1. Usługa stałej bezpośredniej ochrony fizycznej nieruchomości zabudowanej i mienia w obiekcie Zamawiającego oraz obsługa portierni i dozór dzienny w budynku biurowym będzie wykonywana przez jedną osobę, w dni pracy Zamawiającego w godzinach od 6.30 do 17.30. Wykonawca w ramach realizacji, stałej, bezpośredniej ochrony fizycznej nieruchomości zabudowanej i mienia w obiekcie Zamawiającego, zobowiązany jest do dokonania: w godzinach 6.30 - 6.50:

2.2.1.1. codziennego porannego obchodu wokół budynków Zamawiającego zlokalizowanych przy ul. Wrocławskiej 170 G, 170 F i 170 C, (trzykondygnacyjny budynek biurowy budynek G, pomieszczenia magazynowe i garaże murowane - budynek F, monitorowane elektronicznie w zakresie ochrony przed włamaniem i pożarem przez system alarmowy z funkcją automatycznego informowania stacji monitoringu oraz pomieszczenia magazynowe – budynek C);

2.2.1.2. wyłączania systemu alarmowego w dniach pracy Zamawiającego o godzinie 6.30;

2.2.1.3. otwarcia drzwi wejściowych oddziału umożliwiając rozpoczęcie pracy służbom sprzątającym;

2.2.1.4. podejmowania wszelkich czynności i użycia wszelkich środków zmierzających do zapobieżenia przestępstwom, których następstwem byłyby straty w mieniu Zamawiającego, a także do przeciwdziałania powstaniu lub zwiększeniu szkód wynikających ze zdarzeń mających wpływ na bezpieczeństwo obiektu Zamawiającego, zarówno przed przybyciem odpowiednich służb, jak i później;

2.2.1.5. zawiadamiania upoważnionych osób o zaistniałych zagrożeniach i zdarzeniach;

2.2.1.6. prowadzenia „Książki zdarzeń w chronionym obiekcie”, w tym ewidencjonowania czasu i sposobu wykonywania ochrony, wg wzoru zaakceptowanego przez Zamawiającego, w której odnotowane będą wszelkie zdarzenia mające wpływ na stan bezpieczeństwa obiektu.

2.2.2. Wykonawca w ramach realizacji stałej obsługi portierni i dozoru dziennego w budynku biurowym Zamawiającego, zobowiązany jest do dokonania: (w godzinach 6.50 - 17.05):

- 2.2.2.1. obsługi portierni w dniach pracy Zamawiającego w godzinach od 6.50 do 17.05;
- 2.2.2.2. przyjmowania i wydawania osobom upoważnionym wskazanym w „Wykazie osób upoważnionych do pobierania kluczy” oraz przechowywania kluczy do pomieszczeń biurowych w gablocie na klucze, wydawanie kluczy odbywać się będzie za własnoręcznym wpisem osoby pobierającej klucz oraz pracownika Wykonawcy w przypadku przyjęcia kluczy, w rejestrze „Ewidencja wydawanych kluczy”;
- 2.2.2.3. informowania upoważnionego pracownika biura Oddziału Regionalnego wskazanego przez Zamawiającego o każdorazowym zamiarze opuszczenia miejsca wykonywania pracy;
- 2.2.2.4. zapewnienia interwencji patrolu Wykonawcy w ciągu czasu określonego w pkt.2.1.3.2.3 liczonego od chwili powzięcia informacji o sytuacji wymagającej reagowania używając przycisku napadowego lub łącząc się telefonicznie ze stacją monitoringu.

2.2.3. Wykonawca w ramach realizacji stałej, bezpośredniej ochrony fizycznej nieruchomości zabudowanej i mienia w obiekcie Zamawiającego, zobowiązany jest do dokonania w godzinach 17.05 - 17.30:

- 2.2.3.1. codziennego popołudniowego obchodu wokół budynków Zamawiającego zlokalizowanych przy ul. Wrocławskiej 170 G, 170 F; i 170 C;
- 2.2.3.2. uzbrojenia systemu alarmowego w dniach pracy Zamawiającego o godzinie 17.30;
- 2.2.3.3. podejmowania wszelkich czynności i użycia wszelkich środków zmierzających do zapobieżenia przestępstwom, których następstwem byłyby straty w mieniu Zamawiającego, a także do przeciwdziałania powstaniu lub zwiększeniu szkód wynikających ze zdarzeń mających wpływ na bezpieczeństwo obiektu Zamawiającego, zarówno przed przybyciem odpowiednich służb, jak i później;
- 2.2.3.4. zawiadamiania upoważnionych osób o zaistniałych zagrożeniach i zdarzeniach;
- 2.2.3.5. prowadzenia „Książki zdarzeń w chronionym obiekcie”, w tym ewidencjonowania czasu i sposobu wykonywania ochrony, wg wzoru zaakceptowanego przez Zamawiającego, w której odnotowane będą wszelkie zdarzenia mające wpływ na stan bezpieczeństwa obiektu.

2.2.4. W ramach realizacji zamówienia w zakresie usługi stałej bezpośredniej ochrony fizycznej nieruchomości zabudowanej i mienia w obiekcie Zamawiającego oraz

obsługi portierni i dozoru dziennego w budynku biurowym, Wykonawca zobowiązany będzie również do:

- 2.2.4.1. wykonywania umowy za pomocą osób, posiadających wiedzę i doświadczenie w zakresie wykonywania czynności w ramach usługi stałej bezpośredniej ochrony fizycznej nieruchomości i mienia oraz obsługi portierni i dozoru dziennego w budynku Opolskiego Oddziału Regionalnego ARiMR oraz kwalifikacje określone przepisami regulującymi ochronę mienia;
- 2.2.4.2. zapewnienia osobom zatrudnionym przy wykonywaniu przedmiotu umowy umundurowania i oznakowania (identyfikatory) umożliwiającego ich identyfikację, a także środków przymusu bezpośredniego, dozwolonych obowiązujących prawem;
- 2.2.4.3. całodzienny nadzór nad pracownikami ochrony przez uprawnionego przedstawiciela Wykonawcy, posiadającego wpis na listę kwalifikowanych pracowników ochrony fizycznej prowadzoną przez Komendanta Głównego Policji;
- 2.2.4.4. Wykonawca powinien posiadać bezpośredni numer zgłoszeniowy umożliwiający natychmiastowy kontakt ze stacją monitorowania (np. numer infolinii);
- 2.2.4.5. całodziennie wsparcie pracownika ochrony fizycznej przez dwie dyżurujące grupy interwencyjne dla ochrony obiektów przy ul. Wrocławskiej 170 G, 170 F i 170 C z czasem dojazdu do chronionego obiektu nie przekraczającym określonego w pkt.2.1.3.2.3. wszelkie koszty wsparcia (w tym dyżurowanie, dojazd, czas interwencji) wliczone w wynagrodzenie dla pkt.2.2;
- 2.2.4.6. kontrolowania, ustalania i niezwłocznego powiadamiania Zamawiającego na piśmie o stwierdzonych uchybieniach w zabezpieczeniu technicznym obiektu;
- 2.2.4.7. w przypadku zdarzeń stanowiących zagrożenie dla ludzi i mienia zobowiązany jest z zachowaniem bezpieczeństwa, do dokonania czynności mających na celu zapobieżenie zagrożenia lub zmniejszenie zagrożenia, zapobieżenia szkodzie lub jej zmniejszenie, zatrzymania osób a także niezwłocznego zawiadomienia odpowiednich służb publicznych, na okoliczność tych zdarzeń Wykonawca winien sporządzić protokół.

2.3. Przeglądy okresowe urządzeń i systemów.

2.3.1. Wykonawca zobowiązany jest do dokonywania konserwacji i przeglądów wszystkich systemów (alarmowych / przeciwpożarowych / kontroli dostępu / monitoringu wizyjnego we wszystkich obiektach zajmowanych przez Zamawiającego) raz na 3 miesiące, tj. rozpoczęte najpóźniej w ostatnim dniu upływającego kwartału, w którym wymagana była konserwacja. Powyższe zostanie potwierdzone protokołem

*podpisanym przez przedstawicieli stron wg załącznika nr 12 do SWZ
oraz uwidocznione w książce przeglądów konserwacji wg załącznika nr 13 do SWZ.*

2.3.2. Wykonawca w ramach przeglądu technicznego i konserwacji systemu alarmowego zobowiązuje się do:

- 2.3.2.1. sprawdzenia prawidłowości funkcjonowania systemu alarmowego oraz sprawdzenia toru transmisji do SMA,
- 2.3.2.2. sprawdzenia ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
- 2.3.2.3. sprawdzenia poprawności działania akustycznych, optycznych zewnętrznych i wewnętrznych sygnalizatorów alarmowych,
- 2.3.2.4. sprawdzenia i czyszczenia czujników systemu,
- 2.3.2.5. dokonania wszystkich innych czynności nie wymienionych powyżej, a wynikających z dokumentacji technicznej urządzeń i wymaganych przez ich producenta.

2.3.3. Wykonawca w ramach przeglądu technicznego i konserwacji systemów kontroli dostępu (SKD) zobowiązuje się do;

- 2.3.3.1. sprawdzenie prawidłowości działania elektro zaczepów i elektrozawór zainstalowanych na drzwiach z kontrolowanym przejściem,
- 2.3.3.2. sprawdzenia ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
- 2.3.3.3. aktualizacji oprogramowania na stacji roboczej z zainstalowaną aplikacją do zarządzania SKD.

2.3.4 Wykonawca w ramach przeglądu technicznego i konserwacji systemów monitoringu wizyjnego zobowiązuje się do;

- 2.3.4.1 sprawdzenia prawidłowości funkcjonowania systemu wizyjnego,
- 2.3.3.4. sprawdzenia ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
- 2.3.3.5. sprawdzenia poprawności działania,
- 2.3.3.6. sprawdzenia i czyszczenia kamer podłączonych do systemu,

- 2.3.3.7. dokonania wszystkich innych czynności nie wymienionych powyżej, a wynikających z dokumentacji technicznej urządzeń i wymaganych przez ich producenta.
- 2.4. Objęte prawem opcji zakupu - Wykonanie przeniesienia systemów do nowej lokalizacji (wraz z okablowaniem obiektu i uruchomieniem systemu) w przypadku zaistnienia konieczności zmiany siedziby obiektu, o czym Zamawiający poinformuje Wykonawcę z wyprzedzeniem w formie pisemnej lub mailem. Za wykonanie powyższych prac Zamawiający zapłaci Wykonawcy wg ceny za roboczogodzinę - zgodnie z ofertą Wykonawcy.
- 2.5. Objęte prawem opcji zakupu - Wykonawca zapewni na zlecenie Zamawiającego dodatkową doraźną ochronę w postaci bezpośredniej ochrony fizycznej rozliczanej roboczogodzinami. Obowiązki ochrony doraźnej są w zakresie opisanym w pkt.2.2 oraz podczas akcji przyjmowania wniosków, protestów itp.
- 2.6. Objęte prawem opcji zakupu - Wykonawca w sytuacji obiektywnie uzasadnionej warunkami świadczenia umowy i kontynuowania rozpoczętej interwencji, o której mowa w pkt. 2.1.3 ponad limit czasowy opłacany w ramach pkt.2.1 z zastrzeżeniem pkt.2.1.3.3, dokona kontynuacji dozoru interwencyjnego rozliczanego roboczogodzinami.
3. Pozostałe istotne wymagania Zamawiającego, co do przedmiotu zamówienia i realizacji umowy zostały zawarte w projektowanych postanowieniach umowy stanowiących załącznik nr 8 do SWZ.

POTWIERDZENIE WYKONANIA ŚWIADCZEŃ W RAMACH PRAWA OPCJI ZAKUPU ZA MIESIĄC / ROKU W OPOLSKIM ODDZIALE REGIONALNYM / BIURZE POWIATOWYM W * Umowa nr/OR08/2023/2308 z dnia ... - ... - 2023 roku		
Tabela nr 1 - Potwierdzenie wykonania świadczenia w zakresie interwencji /ochrony doraźnej (pkt.2.5 i 2.6 załącznika nr 1 do SWZ) w ramach prawa opcji zakupu)**		
IŁOŚĆ WYKONANYCH ROBOCZOGODZIN INTERWENCJI /OCHRONY DORAŻNEJ W ROZLICZANYM MIESIĄCU	ROZLICZANY MIESIĄC	ZAMAWIAJĄCY***
Ilość roboczogodzin, w tym rozpoczętych:	Miesiąc rok	
Tabela nr 2 - Potwierdzenie wykonania świadczenia w zakresie przeniesienia instalacji (pkt.2.4 załącznika nr 1 do SWZ) w ramach prawa opcji zakupu)**		
IŁOŚĆ WYKONANYCH ROBOCZOGODZIN W ROZLICZANYM MIESIĄCU	ROZLICZANY MIESIĄC	ZAMAWIAJĄCY***
Ilość roboczogodzin, w tym rozpoczętych:	Miesiącrok	

Strony umowy Zamawiający i Wykonawca po zbadaniu zakresu ww. przeprowadzonych prac dokonały ich odbioru:

ZAMAWIAJĄCY:

WYKONAWCA:

.....

.....

(*) — niepotrzebne skreślić

(**) - formularz potwierdzenia wypełnia się tylko w sytuacji, jeśli świadczenie było realizowane w miesiącu, którego dotyczy potwierdzenie

(***) - podpis kierownika BP, jeśli potwierdzenie składa BP / podpis osoby odpowiedzialnej za nadzór nad wykonaniem świadczenia w OR jeśli potwierdzenie składa OR.

ZGŁOSZENIE POTRZEBY WYKONANIA CZYNNOŚCI W RAMACH PRAWA OPCJI ZAKUPU

UMOWA NR Z DNIA

W imieniu Zamawiającego:

Opolski Oddział Regionalny / Biuro Powiatowe* w
Agencji Restrukturyzacji i Modernizacji Rolnictwa

Wykonawca:

.....
Nazwa Wykonawcy

**Opis zdarzenia wymagającego dokonania czynności ochrony doraźnej, przyjazdu grupy interwencyjnej/
przeniesienia instalacji monitoringu do innego budynku/*:**

Termin wykonania / czas reakcji*:

Miejsce wykonania:

* Niepotrzebne skreślić

.....
Data i podpis osoby decyzyjnej w Oddziale Regionalnym / Biurze Powiatowym
upoważnionej przez Zamawiającego

Książka odbiorów świadczeń jednorazowych w ramach czynności: ochrony doraźnej, przyjazdu grupy interwencyjnej/ przeniesienia instalacji monitoringu do innego budynku/ (*) w Oddziale Regionalnym / Biurze Powiatowym (*) do umowy nr z dnia

Lp.	Data i godzina zgłoszenia do Wykonawcy potrzeby wykonania świadczenia	Data i godzina przybycia Wykonawcy celem wykonania świadczenia	Przedmiot prac	Ilość stwierdzonych przez Zamawiającego interwencji / roboczogodzin / usług Wykonawcy w momencie należytego zakończenia świadczenia	Podpis pracownika Zamawiającego stwierdzającego należyte wykonanie świadczenia	Podpis wykonującego świadczenie w imieniu Wykonawcy

* niepotrzebne skreślić

WYKAZ UPOWAŻNIONYCH KONTAKTÓW

(Wypełnia Kierownik Biura lub osoba upoważniona)

OBIEKT	
ADRES:	
TELEFON	

1. Wykaz osób do powiadomienia w przypadku powstania alarmu:

Nazwisko i Imię	Funkcja	Telefon	Uwagi

2. Czasy załączania i wyłączania lokalnego systemu alarmowego:

Dzień tygodnia	Godzina załączenia*	Godzina wyłączenia**	Uwagi
Poniedziałek			
Wtorek			
Środa			
Czwartek			
Piątek			
Sobota	-----	-----	Wyjątek stanowi praca zlecona w tym dniu o czym operator SMA zostanie wcześniej powiadomiony
Niedziela	-----	-----	

* Godzina załączenia alarmu adekwatna z zamknięciem biura + 30 min.

** Godzina wyłączenia alarmu adekwatna z otwarciem biura – 30 min.

3. Hasło odwołania alarmu:

4. Informacje dodatkowe:

.....
.....
.....

Zamawiający:

Wykonawca:

Informacje dotyczące przetwarzania danych osobowych

Wypełniając obowiązek wynikający z art. 13 lub/i art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [Dz. Urz. UE L 119 z 27.04.2016 r., str. 1] – (dalej zwane Rozporządzeniem), informujemy, że:

- 1) administratorem Pani/Pana danych osobowych jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa;
- 2) z administratorem danych osobowych może Pani/Pan kontaktować się poprzez adres e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa, ul. Poleczki 33, 02-822 Warszawa;
- 3) administrator danych wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl, lub pisemnie na adres korespondencyjny administratora danych, wskazany w pkt 2;
- 4) zebrane dane osobowe będą przetwarzane przez administratora danych na podstawie art. 6 ust. 1 lit. a) Rozporządzenia, czyli na podstawie udzielonej zgody na przetwarzanie danych osobowych w postaci: imienia i nazwiska pracownika, prywatnego numeru telefonu przekazywanych wykonawcy usługi polegającej na całodobowej ochronie obiektów w Opolskim Oddziale Regionalnym i Biurach Powiatowych ARiMR (przekazanie w celu powiadamiania o sygnałach naruszenia bezpieczeństwa obiektu i upoważnienia do rozbrajania alarmu w biurze lub oddziale ARiMR);
- 5) zebrane dane osobowe mogą być udostępniane podmiotom publicznym uprawnionym do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa oraz podmiotom przetwarzającym dane osobowe na zlecenie administratora w związku z wykonywaniem powierzonego im zadania w drodze zawartej umowy (np. dostawcom IT, usług ochroniarskich, monitoringu);
- 6) przetwarzanie danych następujące na podstawie zgody trwa do jej odwołania;
- 7) przysługuje Pani/Panu prawo dostępu do Pani/Pana danych, prawo żądania ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, w przypadkach określonych w Rozporządzeniu;
- 8) dane nie będą transferowane do państw trzecich i organizacji międzynarodowych;
- 9) w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy Rozporządzenia, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie: imienia i nazwiska oraz prywatnego numeru telefonu w celu przekazania ich do Wykonawcy usługi polegającej na całodobowej ochronie obiektów w Opolskim Oddziale Regionalnym i Biurach Powiatowych ARiMR, zgodnie z Rozporządzeniem 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 oraz zgodnie z klauzulą informacyjną dołączoną do mojej zgody.

.....

Miejscowość, data,

.....
czytelny podpis pracownika

Instrukcja

Postępowania w przypadku obsługi systemu alarmowego podłączonego do Stacji

Monitorowania Alarmów

1. Przed uzbrojeniem lokalnego systemu alarmowego należy sprawdzić stan obiektu:
 - ✓ zamknąć wszystkie okna,
 - ✓ wyłączyć urządzenia elektryczne (z wyjątkiem niezbędnych do pozostawienia, np. fax, urządzenia w serwerowni, itp.)
 - ✓ sprawdzić czy w obiekcie nie znajdują się inne osoby lub zwierzęta (pies, kot, ptak). Naruszenie w/w zasad może być przyczyną fałszywego alarmu.

2. Osoba odpowiedzialna za obsługę lokalnego systemu alarmowego powinna umieć:
 - ✓ określić stan pracy urządzeń w tym posiadać umiejętności odczytu pamięci zdarzeń,
 - ✓ zmienić samodzielnie kod,
 - ✓ uzbroić lokalny system alarmowy z pominięciem linii.

3. Załączenie i wyłączenie lokalnego systemu alarmowego, rejestrowanie przez Stację Monitorowania Alarmów (SMA) i wywołujące automatycznie reakcje ochronne, następować musi tylko w godzinach i na warunkach określonych w załączniku nr 10 do SWZ (z tolerancją plus minus 30 minut). Operacje te dokonywane być powinny, wyłącznie przez osobę upoważnioną przez użytkownika obiektu. W przypadku jednorazowych zmian godzin załączania lokalnego systemu alarmowego należy o tym fakcie powiadomić operatora SMA tel. serwisowy, który telefonicznie sprawdzi prawdziwość zgłoszenia.

4. W przypadku zmiany godzin załączania i wyłączenia systemu alarmowego na inne, niż ustalone w pkt.2 załącznika nr 10 do SWZ, konieczne jest powiadomienie Wykonawcy w formie pisemnej lub mailowej (email:

5. Każde wyłączenie lokalnego systemu alarmowego, bez uprzedniego poinformowania operatora SMA, poza godzinami określonymi w pkt.2 załącznika nr 10 do SWZ traktowane będzie jako wywołanie alarmu powodujące telefoniczne sprawdzenie sytuacji w obiekcie przez Operatora SMA. W przypadku braku możliwości wcześniejszego powiadomienia operatora SMA należy ten fakt zgłosić bezzwłocznie po wejściu podając dla celów identyfikacyjnych:
 - ✓ nazwę i adres obiektu;
 - ✓ imię i nazwisko osoby zgłaszającej;
 - ✓ hasło identyfikacyjne (hasło odwołania alarmu).

W przypadku braku określenia godzin załączenia i wyłączenia lokalnego systemu alarmowego każde poprawne jego załączenie lub wyłączenie traktowane będzie jako dokonane przez osobę upoważnioną. W takim przypadku nie będą podejmowane żadne czynności.

6. W przypadku wystąpienia alarmu spowodowanego naruszeniem linii wejściowej i wyłączeniu go za pomocą prawidłowego kodu należy bezzwłocznie powiadomić o tym fakcie operatora SMA podając dla celów identyfikacji:
 - ✓ nazwę i adres obiektu
 - ✓ imię i nazwisko osoby zgłaszającej,
 - ✓ hasło identyfikacyjne (hasło odwołania alarmu)

W przypadku braku takiego zgłoszenia, operator SMA podejmuje próbę skontaktowania się z użytkownikiem lokalnego systemu alarmowego w celu potwierdzenia stanu obiektu.

*Załącznik nr 11 do SWZ, stanowiący Załącznik nr 8
do projektowanych postanowień umownych
(BOR08.2619.2.2023.DP)*

7. W godzinach monitorowania obiektu, przynajmniej jedna osoba upoważniona do powiadomienia o zaistniałym alarmie, powinna przebywać w miarę możliwości w miejscu wskazanym w ankiecie zgłoszeniowej i w przypadku wystąpienia alarmu na żądanie operatora SMA przybyć do obiektu w czasie nie dłuższym niż 40 minut.

8. W sprawach nietypowych i budzących wątpliwości należy skontaktować się z operatorem SMA tel. lub służbą techniczną tel.

Zamawiający:

Wykonawca:

Nazwa jednostki:

**PROTOKÓŁ KONSERWACJI / NAPRAWY SYSTEMU ALARMOWEGO
I PRZECIWPOŻAROWEGO ORAZ SYSTEMU KONTROLI DOSTĘPU I MONITORINGU
WIZYJNEGO**

W dniu Wykonawca dokonał konserwacji systemu.

Czynności wykonane przez konserwatora:

Lp.	Wykonane czynności przeglądu	Wynik pozytywny*	Wynik negatywny*	Uwagi:
Przeгляд techniczny i konserwacja systemu alarmowego / przeciwpożarowego				
1	sprawdzenie prawidłowości funkcjonowania systemu alarmowego oraz sprawdzenia toru transmisji do SMA			
2	sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego			
3	sprawdzenie poprawności działania akustycznych, optycznych zewnętrznych i wewnętrznych sygnalizatorów alarmowych			
4	sprawdzenie i czyszczenia czujników systemu			
5	dokonanie wszystkich innych czynności nie wymienionych powyżej, a wynikających z dokumentacji technicznej urządzeń i wymaganych przez ich producenta			
Przeгляд techniczny i konserwacja systemu kontroli dostępu (SKD)				
1	sprawdzenie prawidłowości działania elektro zaczepów i elektrozwór zainstalowanych na drzwiach z kontrolowanym przejściem			
2	sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego			
3	aktualizacja oprogramowania na stacji roboczej z zainstalowaną aplikacją do zarządzania SKD			
Przeгляд techniczny i konserwacja systemu monitoringu wizyjnego				
1	sprawdzenie prawidłowości funkcjonowania systemu wizyjnego			
2	sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego			
3	sprawdzenie poprawności działania			
4	sprawdzenie i czyszczenia kamer podłączonych do systemu			
5	dokonanie wszystkich innych czynności nie wymienionych powyżej, a wynikających z dokumentacji technicznej urządzeń i wymaganych przez ich producenta			

* w poniższej tabeli wstawiamy znak „X”

Uwagi i zalecenia dla użytkownika:

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach - po jednym dla każdej ze stron.

Zamawiający:

(data i czytelny podpis przedstawiciela Zamawiającego)

Wykonawca:

(data i czytelny podpis przedstawiciela Wykonawcy)

**KSIĄŻKA PRZEGLĄDÓW I KONSERWACJI / NAPRAW SYSTEMÓW ALARMOWYCH
I PRZECIWPOŻAROWYCH ORAZ SYSTEMU KONTROLI DOSTĘPU I MONITORINGU
WIZYJNEGO**

OBIEKT:

.....
.....
.....
.....
.....

LP.	DATA	ZAKRES WYKONANYCH PRAC	PODPIS KONSERWATORA	PODPIS POŚWIADCZAJĄCEGO	UWAGI
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					

ZGŁOSZENIE AWARII

NAZWA WYKONAWCY:	ADRES WYKONAWCY:	DANE KONTAKTOWE WYKONAWCY
------------------	------------------	------------------------------

ZGŁASZAJĄCY:

NAZWA FIRMY:	Opolski Oddział Regionalny Agencji Restrukturyzacji i Modernizacji Rolnictwa w Opolu				
ADRES:	ul. Wrocławska 170G, 45-836 Opole				
NAZWISKO OSOBY ZGŁASZAJĄCEJ W OOR ARIMR:		TELEFON:		E-MAIL:	
DATA ZGŁOSZENIA:			GODZINA ZGŁOSZENIA:		

MIEJSCE WYSTĄPIENIA AWARII:

NAZWA OBIEKTU ZAMAWIAJĄCEGO:	Opolski Oddział Regionalny / Biuro Powiatowe* ARiMR w				
ADRES:					
NAZWISKO KIEROWNIKA OBIEKTU LUB OSOBY UPOWAZNIONEJ:		TELEFON:		E-MAIL:	
NAZWA USZKODZONEGO URZĄDZENIA		TYP / MODEL		PRODUCENT	
NUMER SERYJNY URZĄDZENIA				DATA ZAKUPU	
OPIS AWARII					

DATA, PIECZĄTKA I PODPIS OSOBY ZGŁASZAJĄCEJ

* niepotrzebne skreślić

**Zgłoszenie potrzeby przeniesienia instalacji monitoringu do innego budynku :
na podstawie § umowy nr**

NAZWA WYKONAWCY:	ADRES WYKONAWCY:	DANE KONTAKTOWE WYKONAWCY
------------------	------------------	------------------------------

ZGŁASZAJĄCY:

NAZWA FIRMY:	Opolski Oddział Regionalny Agencji Restrukturyzacji i Modernizacji Rolnictwa w Opolu				
ADRES:	ul. Wrocławska 170G, 45-836 Opole				
NAZWISKO OSOBY ZGŁASZAJĄCEJ W OOR ARIMR:		TELEFON:		E-MAIL:	
DATA ZGŁOSZENIA:			GODZINA ZGŁOSZENIA:		

Dane dot. zgłaszanej usługi:

ZAKRES I OPIS INSTALACJI DO PRZENIESIENIA	
MIEJSCE DEMONTAŻU INSTALACJI:	
MIEJSCE INSTALACJI:	
TERMIN REALIZACJI ZLECENIA	
UWAGI:	

DATA, PIECZĄTKA I PODPIS OSOBY ZGŁASZAJĄCEJ

* niepotrzebne skreślić

**Umowa powierzenia Wykonawcy przetwarzania danych osobowych
zawarta w dniu 2023 r. w Opolu
(dalej zwana także – „Umową Powierzenia”)**

pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, adres: 00-175 Warszawa, Aleja Jana Pawła II 70, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną w dalszej części umowy „**Zamawiającym**” lub „**Administratorem**”,

reprezentowaną przez:

Pana Wojciecha Komarzyńskiego - Dyrektora Opolskiego Oddziału Regionalnego ARiMR w Opolu;

a

....., zwanym dalej „**Wykonawcą**” lub „**Przetwarzającym**”,

reprezentowanym(a) przez:

.....

Zamawiający i Wykonawca w dalszej części niniejszej Umowy Powierzenia zwani są także pojedynczo „**Stroną**” i łącznie „**Stronami**”.

Zważywszy, że w dniu2023 r., Strony zawarły umowę nr (zwaną dalej: „Umową Podstawową”) oraz mając na uwadze fakt, że w związku z wykonywaniem Umowy Podstawowej mogą być przetwarzane przez Przetwarzającego dane osobowe, Strony postanawiają, co następuje:

§ 1

Oświadczenia stron.

1. Administrator oświadcza, że jest Administratorem oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Przetwarzający oświadcza, że w ramach prowadzonej działalności profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym niniejszą umową i Umową Podstawową, oraz że posiada i stosuje w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego jej wykonania. Przetwarzający oświadcza, że znane są mu przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – zwanym dalej „Rozporządzeniem” lub „RODO”, w szczególności w zakresie obowiązków Podmiotu Przetwarzającego, którego obowiązki na mocy niniejszej umowy przyjmuje. Przetwarzający zapewnia, że daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia (oraz innych obowiązujących w tym zakresie przepisów prawa) i chroniło prawa osób, których dane dotyczą.
3. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. W szczególności zobowiązuje się przekazać Administratorowi niezwłocznie **nie później niż w terminie 24 godzin** informacje o stosowanych środkach zabezpieczenia danych osobowych, przypadkach naruszenia ochrony danych osobowych od zaistnienia incydentu oraz zawiadomienia o tym osob, których dane osobowe dotyczą, o ile zażąda tego Administrator. Nadto zobowiązuje się on udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków administratora określone w RODO oraz umożliwić Administratorowi lub audytorowi przez niego upoważnionemu przeprowadzanie audytów, w tym inspekcji. Przetwarzający zobowiązuje się do stosowania się do zaleceń Administratora dotyczących

zasad przetwarzania powierzonych danych osobowych oraz dotyczących poprawy zabezpieczenia danych osobowych, sporządzonych w wyniku kontroli przeprowadzonych przez Administratora lub upoważnionego przez niego audytora.

§ 2

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Przetwarzającemu, w trybie art. 28 Rozporządzenia dane osobowe do przetwarzania wyłącznie w celach związanych z realizacją niniejszej Umowy i Umowy Podstawowej i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów na podstawie udokumentowanego polecenia Administratora. Przetwarzanie danych osobowych następowało będzie w formie papierowej, jak również przy wykorzystaniu systemów informatycznych.
2. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą. W celu wykonania Umowy Podstawowej i Umowy Powierzenia, Zamawiający powierza Wykonawcy w trybie art. 28 RODO przetwarzanie danych osobowych ze zbioru Zamawiającego zawartych w dokumentacji utrwalonej w formie pisemnej, a Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.
3. Zamawiający powierza Wykonawcy przetwarzanie danych osobowych poprzez wykonanie następujących operacji na powierzonych danych osobowych:
 - a. przechowywania w formie dokumentu w formie papierowej, zawiadomienia o imionach i nazwiskach wraz z numerami telefonów osób uprawnionych do odwoływania alarmów w poszczególnych jednostkach terenowych Zamawiającego,
 - b. dostępu do danych (imion i nazwisk) osób upoważnionych do pobierania kluczy do pomieszczeń biurowych w siedzibie Opolskiego Oddziału Regionalnego w ramach obsługi portierni oraz dozoru dziennego w siedzibie OR,
 - c. dostępu do danych (imion i nazwisk) osób uprawnionych do dezaktywacji alarmów zawartych w systemach alarmowych, systemach kontroli dostępu – w szczególności w trakcie przeprowadzania konserwacji systemów przez uprawnionych pracowników Wykonawcy,
 - d. przechowywanie w formie elektronicznej na komputerze stacjonarnym powierzonych danych jedynie w czasie i celu wykonania usługi;
 - e. usuwanie powierzonych danych osobowych z pamięci komputera po wykonaniu przedmiotu umowy;
 - f. dostępu do wizerunków osób fizycznych w postaci danych monitoringu wizyjnego – jedynie w trakcie i w celu konserwacji, naprawy sprzętu, bez możliwości utrwalania przedmiotowych danych;

§ 3

Obowiązki Przetwarzającego

1. Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

2. Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy - „EOG”). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują dane poza EOG.
3. 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 RODO.
4. Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
5. Przetwarzający pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych.
6. Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych niezwłocznie nie później niż w ciągu 12 godzin od jego wykrycia informuje o tym zdarzeniu Administratora. Zawiadomienie o stwierdzeniu naruszenia powinno zostać przesłane Administratorowi wraz z niezbędną dokumentacją odnoszącą się do naruszenia – w szczególności opisującą charakter naruszenia ochrony danych osobowych, jego skalę, możliwe konsekwencje naruszenia ochrony danych, czas zdarzenia, osoby odpowiedzialne i osoby poszkodowane – celem umożliwienia Administratorowi spełnienia obowiązku powiadomienia organu nadzoru.
7. Wykonawca zobowiązuje się zastosować środki ochrony kryptograficznej wobec urządzeń przenośnych takich jak: laptop, smartfon, pendrive, tablet, przenośny dysk twardy oraz innych rodzajów przenośnej pamięci masowej, jeśli będą one wykorzystywane do przetwarzania powierzonych danych osobowych, bądź innych danych dotyczących Administratora danych.

§ 4

Obowiązki Administratora

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 5

Bezpieczeństwo danych

1. Przetwarzający zapewnia, iż przeprowadził analizę ryzyka przetwarzania powierzonych danych i stosuje stosownie do jej wyników, organizacyjne i techniczne środków ochrony danych.
2. Na żądanie Przetwarzający przedstawi Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Kopie przedstawionych dokumentów i dowody przedstawienia informacji, Administrator przechowuje dla potrzeb spełnienia wymogu rozliczalności.

3. Przetwarzający zobowiązuje się spełnić warunki w tym podjąć środki zabezpieczające powierzone dane osobowe, w szczególności Wykonawca zobowiązuje się do:
 - a. zapewnienia kontroli nad prawidłowością przetwarzania powierzonych danych osobowych,
 - b. zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia powierzonych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
 - c. dopuszczenia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania powierzonych danych osobowych wyłącznie osób posiadających wydane przez niego upoważnienie,
 - d. prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania powierzonych danych osobowych,
 - e. zapewnienia, aby osoby upoważnione do przetwarzania powierzonych danych osobowych zachowały je w tajemnicy także po wygaśnięciu niniejszej Umowy Powierzenia, między innymi poprzez poinformowanie tych osób o prawnych konsekwencjach naruszenia poufności powierzonych danych osobowych i wykorzystania tych danych niezgodnie z przeznaczeniem oraz odebranie od tych osób oświadczeń o zachowaniu w tajemnicy wskazanych danych osobowych,
 - f. niewykorzystywania powierzonych danych osobowych dla celów innych niż wykonywanie Umowy Podstawowej i Umowy,

§ 6

Nadzór nad wykonywaniem Umowy Powierzenia.

1. Administrator w oparciu o art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Zamawiający jest uprawniony do kontrolowania sposobu wykonywania Umowy Powierzenia przez Wykonawcę. Ponadto Zamawiający ma prawo kontrolowania, czy Wykonawca przetwarzając powierzone dane osobowe przestrzega przepisów RODO, Ustawy, wydanych do niej rozporządzeń oraz innych mających zastosowanie przepisów w zakresie, w jakim ewentualne naruszenie tych przepisów mogłoby prowadzić do ponoszenia odpowiedzialności przez Zamawiającego, w tym zagrażało bezpieczeństwu powierzonych danych osobowych lub naruszało prawa osób trzecich.
3. W celu wykonania kontroli upoważnieni pracownicy Zamawiającego mają prawo:
 - a. wstępu do obszarów przetwarzania powierzonych danych osobowych (m.in. pomieszczeń), w których jest przetwarzany zbiór danych osobowych, oraz w których przetwarzane są dane osobowe poza zbiorem i przeprowadzania czynności kontrolnych,
 - b. żądania od Wykonawcy udostępnienia dokumentów, złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,

- c. przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych Wykonawcy służących do przetwarzania powierzonych danych osobowych,
4. Z czynności kontrolnych przeprowadzający kontrolę pracownicy Zamawiającego sporządzają protokół w dwóch egzemplarzach, z których jeden egzemplarz doręcza się kontrolowanemu.
 5. Wykonawca zapewnia możliwość niezwłocznego przeprowadzenia czynności kontrolnych przez Zamawiającego w każdym z obszarów przetwarzania powierzonych danych osobowych. Osoby uprawnione do przeprowadzenia kontroli mają prawo niezwłocznego wstępu do obszarów przetwarzania powierzonych danych osobowych, w dniach i w godzinach wykonywania pracy u Wykonawcy, na ustne żądanie skierowane do osób zapewniających ochronę fizyczną wraz z okazaniem upoważnienia do przeprowadzenia kontroli.
 6. W przypadku ujawnienia okoliczności uznanych przez Zamawiającego za nieprawidłowości w zakresie wykonywania Umowy Powierzenia, Ustawy lub RODO, Wykonawca zobowiązuje się do ich usunięcia w wyznaczonym przez Zamawiającego terminie.
 7. W razie niezastosowania się przez Wykonawcę do wydanych mu poleceń w tym m.in. w przypadku nieusunięcia przez Wykonawcę wskazanej mu nieprawidłowości w wyznaczonym terminie, Zamawiający może naliczyć Wykonawcy karę umowną w wysokości 1 000,00 zł (słownie: jeden tysiąc złotych) za każdy przypadek stwierdzonej i nieusuniętej w terminie nieprawidłowości.
 8. Jeżeli nieprawidłowości wskazane w ust. 6 zostaną ponownie ujawnione, Zamawiający może naliczyć Wykonawcy karę umowną w wysokości wskazanej w ust. 7 bez wyznaczania terminu do usunięcia tych nieprawidłowości.
 9. W przypadku stwierdzenia nieuprawnionego udostępnienia przez Wykonawcę powierzonych danych, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1 000,00 zł (słownie: jeden tysiąc złotych) za każdy przypadek nieuprawnionego udostępnienia powierzonych danych.
 10. W przypadku naliczenia kary umownej, Zamawiający wezwie Wykonawcę do zapłaty kary umownej w terminie 14 dni od dnia doręczenia pisemnego wezwania do jej zapłaty.

§ 7

Dalsze powierzenie danych do przetwarzania

1. Przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podmiotom przetwarzającym jedynie w celu wykonania umowy tylko i wyłącznie po uzyskaniu uprzedniej pisemnej zgody Administratora. Administrator po wyrażeniu zgody będzie w stosunku do podmiotów przetwarzających korzystał ze swoich uprawnień względem Przetwarzającego wynikających z niniejszej Umowy Powierzenia, w tym uprawnień wynikających z §6.
2. Podmioty przetwarzające, o którym mowa ust. 1 muszą spełniać te same gwarancje i obowiązki jakie zostały nałożone na Przetwarzającego w niniejszej umowie.

3. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podmiotach przetwarzających obowiązków ochrony danych.

§ 8

Odpowiedzialność Przetwarzającego

1. 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. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.
3. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa. Przetwarzający będzie zobowiązany do bezzwłocznego zwrotu kwot poniesionych przez Administratora tytułem nałożonych na niego kar z tytułu niedopełnienia przez Przetwarzającego obowiązków wynikających z niniejszej Umowy oraz RODO - na każdego jego żądanie w terminie 7 dni od dnia otrzymania takiego żądania.

§ 9

Przetwarzanie powierzonych danych osobowych po wygaśnięciu Umowy Powierzenia.

1. Umowa Powierzenia wygasa z chwilą wykonania Umowy Podstawowej.
2. W przypadku rozwiązania, wygaśnięcia, unieważnienia lub odstąpienia od Umowy Podstawowej, Wykonawca zobowiązuje się niezwłocznie, nie później jednak niż w terminie 3 dni kalendarzowych od dnia wystąpienia tej okoliczności w godzinach pracy Zamawiającego, zwrócić wszelkie powierzone mu na podstawie Umowy Powierzenia dane osobowe. Jeżeli przekazane dane osobowe zostały w jakikolwiek sposób utrwalone w wersji elektronicznej Wykonawca jest zobowiązany skutecznie usunąć te dane z nośników elektronicznych pozostających w jego dyspozycji.
3. Powierzenie przetwarzania danych osobowych trwa do upływu terminu wskazanego w ust. 1 lub 2.
4. Celem usunięcia wątpliwości Strony ustalają, że pomimo wygaśnięcia Umowy Powierzenia zachowują moc obowiązującą wszelkie postanowienia nakładające lub mogące nałożyć na Wykonawcę jakiegokolwiek zobowiązanie względem Zamawiającego, po terminie wygaśnięcia Umowy Powierzenia, w tym m.in. postanowienia §9 ust. 3 i §9 ust. 6 Umowy Powierzenia.

5. W przypadku niewykonania przez Wykonawcę zobowiązania wynikającego z treści § 9 ust. 3 Umowy Powierzenia Zamawiający uprawniony jest do naliczenia Wykonawcy kary umownej w wysokości 10 000,00 zł (słownie: dziesięć tysięcy złotych). W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia § 6 ust. 10 Umowy Powierzenia.
6. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy Powierzenia powstanie szkoda przewyższająca zastrzeżone kary umowne, o których mowa w niniejszej Umowie Powierzenia, Zamawiającemu, oprócz tej kary, przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z innych przyczyn niż te, ze względu na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych Kodeksu cywilnego.

§ 10

Wykonywanie Umowy Powierzenia.

1. Wynagrodzenie z tytułu wykonania Umowy Powierzenia zawarte jest w wynagrodzeniu przewidzianym dla Wykonawcy w § 5 ust. 1 Umowy Podstawowej.
2. Wykonanie Umowy Powierzenia nie może być podstawą dodatkowych roszczeń Wykonawcy wobec Zamawiającego.
3. Uprawnienie Zamawiającego względem Wykonawcy do kary umownej oraz odszkodowań wskazanych w niniejszej Umowie Powierzenia nie wyłącza odpowiedzialności Wykonawcy w przypadku naruszenia przepisów RODO.
4. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Przetwarzający:
 - a. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
 - b. przetwarza dane osobowe w sposób niezgodny z umową lub RODO;
 - c. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 11

Postanowienia końcowe

1. Wszelkie zmiany Umowy Powierzenia dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą Umową znajdują zastosowanie odpowiednie przepisy Kodeksu Cywilnego, przepisy 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 osobowych oraz uchylenia dyrektywy 95/46/WE ogólne rozporządzenie o ochronie danych: Dz.U. UE.L.2016.119.1 ze zm., ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2019 r. poz. 1781), oraz innych przepisów krajowych dotyczących ochrony danych osobowych.

3. Sądem właściwym dla rozstrzygania sporów powstałych w związku z zawarciem lub wykonywaniem Umowy Powierzenia jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Umowa Powierzenia wchodzi w życie z dniem jej podpisania przez Strony.
5. Umowę Powierzenia sporządzono w czterech jednobrzmiących egzemplarzach: trzy dla Zamawiającego i jeden dla Wykonawcy.

.....
Administrator danych (Zamawiający)

.....
Podmiot przetwarzający (Wykonawca)

.....
(Miejscowość, data)

OŚWIADCZENIE

.....
(Nazwa - firma Wykonawcy)

.....
(Adres Wykonawcy)

.....
(Imię i nazwisko osoby skierowanej do realizacji przedmiotu umowy)

Oświadczam, że zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych i zobowiązuję się do przestrzegania:

- przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.U. UE.L.2016.119.1 ze zm.)
- ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (tj. Dz. U. z 2019 r. poz. 1781)
- polityki Bezpieczeństwa informacji obowiązującej w ARiMR w zakresie wytycznych bezpieczeństwa informacji dla Wykonawców

W związku z powyższym zobowiązuję się do zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji w tym danych osobowych i innych pozyskanych w trakcie realizacji umowy.

.....
(Podpis osoby skierowanej do realizacji usługi)

Wytyczne bezpieczeństwa informacji dla Wykonawców

Bezpieczeństwo Informacji w ARiMR

1. Polityka Bezpieczeństwa Informacji obowiązuje wszystkich wykonawców, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów lub stref informacyjnych Opolskiego Oddziału Regionalnego Agencji Restrukturyzacji i Modernizacji Rolnictwa (Opolski OR ARiMR).
2. Wykonawca zobowiązuje się do przestrzegania przyjętych w ARiMR zasad bezpieczeństwa informacji, których treść jest określona w Polityce Bezpieczeństwa Informacji w ARiMR, a przedstawiona w obecnych wytycznych.
3. Polityka Bezpieczeństwa Informacji w ARiMR dotyczy zasobów materialnych i niematerialnych Agencji i znajduje zastosowanie zarówno do pracowników Agencji, jak i podmiotów zewnętrznych z nią współpracujących lub wykonujących usługi.
4. Wykonawca potwierdza fakt zapoznania się z wytycznymi własnoręcznym podpisem na umowie lub oświadczeniu, przedłożonym przez ARiMR.
5. Wszystkie informacje wrażliwe i środki służące do ich przetwarzania, do których Wykonawca będzie miał dostęp i są własnością Agencji lub są przez nią wykorzystywane, podlegają ochronie.
6. Informacja prawnie chroniona oraz każda informacja, której utrata, ujawnienie lub udostępnienie osobie/podmiotowi nieuprawnionemu mogłoby spowodować szkodę materialną lub niematerialną dla Agencji lub naruszyć prawnie chroniony interes innych osób/podmiotów podlega szczególnej ochronie.
7. W przypadku, gdy Wykonawca przypadkowo wszedł w posiadanie dokumentów lub innych materiałów stanowiących informację prawnie chronioną dla ARiMR, ma obowiązek natychmiastowego przekazania jej Kierownikowi jednostki organizacyjnej lub Inspektorowi Bezpieczeństwa Informacji w ARiMR.
8. Wykonawca zobowiązuje zapoznać pracowników i osoby trzecie realizujące objęte umową zadania, w zakresie zachowania zasad bezpieczeństwa informacji określonych w Wytycznych bezpieczeństwa informacji.
9. Odpowiedzialność za bezpieczeństwo informacji Opolskiego OR ARiMR obejmuje nie tylko siedzibę oddziału i biur powiatowych, ale także wszelkie sytuacje, w których Wykonawca może mieć dostęp do informacji prawnie chronionych będących własnością ARiMR.
10. Informacje związane z działalnością Agencji są przetwarzane także poza jej siedzibą. Obejmuje to także i w szczególności zdalny dostęp do sieci komputerowej Agencji.

Bezpieczeństwo fizyczne i środowiskowe

Strefa administracyjna

1. Strefa administracyjna w ARiMR to powierzchnia będąca w użytkowaniu Agencji i służąca do poruszania się w niej tylko pracowników ARiMR.
2. Na granicach strefy administracyjnej funkcjonuje elektroniczna kontrola dostępu.
3. W Agencji wydzielono obszary dostaw i załadunku dla Wykonawców i jest to strefa obsługi dostępna ogólnie dla Wykonawców i beneficjentów ARiMR.

Strefa bezpieczeństwa

4. Pobyt osoby - Wykonawcy, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany i może się odbywać tylko z osobą posiadającą uprawnienia do tej strefy.
5. Wszelkie prace w strefie bezpieczeństwa wykonywane zarówno przez podmioty nieuprawnione jak i uprawnione do przebywania w strefie bezpieczeństwa mogą się odbywać tylko przy ciągłej obecności osoby uprawnionej do tej strefy
6. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa, musi zostać odnotowany na podstawie dokumentu tożsamości.

Wykonywanie usługi - dostawy na terenie Opolskiego OR

1. Wykonawca może poruszać się w strefie administracyjnej (w obecności uprawnionego pracownika ARiMR), w godzinach: 8.00 - 14.00 w dniach roboczych Agencji.

*Załącznik nr 17 do SWZ, stanowiący Załącznik nr 5
do projektowanych postanowień umownych
(BOR08.2619.2.2023.DP)*

2. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Wykonawcy posiadają identyfikatory z napisem „Gość” i numerem identyfikatora, w które zostaną zaopatrzeni przez pracownika Punktu Obsługi Klienta Opolskiego OR.
3. Wejście osoby - firmy zewnętrznej (administrator obiektu, serwisant, dostawca, firma wykonująca remont, usługę, dostawę) po godzinach pracy Opolskiego OR na teren obiektu jest możliwe jedynie z upoważnionym pracownikiem Opolskiego OR i po wcześniejszym pisemnym wystąpieniu o zgodę na wejście na teren obiektu Opolskiego OR.
4. Zgodę na wejście w/w na teren Opolskiego OR w formie pisemnej wyraża Administrator Zabezpieczeń Fizycznych Opolskiego OR.
5. Pracownik Opolskiego OR odpowiada za pobyt Wykonawcy od momentu wejścia na teren obiektu i przez cały czas wykonywanych przez niego prac, aż do momentu opuszczenia przez niego Opolskiego OR. Wychodząc z siedziby Opolskiego OR, Wykonawca obowiązany jest do zwrotu identyfikatora, a pracownik OR potwierdza w Księżce wejścia/wyjścia do strefy administracyjnej godzinę opuszczenia pomieszczeń jednostki organizacyjnej ARIMR.

Naruszenie bezpieczeństwa informacji

1. Naruszenie postanowień Polityki Bezpieczeństwa Informacji w ARiMR przez Wykonawcę stanowi podstawę do odstąpienia przez Agencję od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
2. Naruszenie przepisów bezpieczeństwa informacji oraz o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w Rozporządzeniu 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/W (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz w Kodeksie karnym.

*Załącznik nr 17 do SWZ, stanowiący Załącznik nr 5
do projektowanych postanowień umownych
(BOR08.2619.2.2023.DP)*

Nazwa Wykonawcy:

.....

Adres Wykonawcy:

.....

**OŚWIADCZENIE WYKONAWCY / PODWYKONAWCY
dotyczące uprawnień pracowników przewidzianych do wykonania zamówienia**

BOR08.2619.2.2023.DP

Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn. „*Usługa ochrony nieruchomości zajmowanych przez Agencję Restrukturyzacji i Modernizacji Rolnictwa w województwie opolskim*”, oświadczam, że osoby które będą uczestniczyć w wykonywaniu przedmiotowego zamówienia posiadają wymagane uprawnienia tj. są wpisane na listę kwalifikowanych pracowników ochrony fizycznej oraz listę kwalifikowanych pracowników zabezpieczenia technicznego, zgodnie z art. 26 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (tj. Dz.U. 2021 poz. 1995).

**ANKIETA – WYMAGANIA DLA PODMIOTU ZEWNĘTRZNEGO
w zakresie możliwości powierzenia przetwarzania danych osobowych**

Poniższa ankieta ma na celu ustalenie czy podmiot zewnętrzny, któremu ARiMR zamierza powierzyć przetwarzanie danych osobowych, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. W tym celu należy odpowiedzieć na poniższe pytania.

1. SYSTEMY OCHRONY DANYCH, KODEKSY POSTĘPOWANIA, CERTYFIKACJA

- 1) Czy Podmiot zewnętrzny ma wdrożony system zarządzania bezpieczeństwem informacji lub znak jakości i oznaczeń w zakresie ochrony danych osobowych, o których mowa w art. 42 RODO, i które obejmują całość operacji przetwarzania danych w ramach realizacji Umowy?

TAK/NIE

- 2) Czy Podmiot zewnętrzny wdrożył i stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO?

TAK/NIE

- 3) Czy system ochrony danych osobowych Podmiotu zewnętrznego był poddawany w ciągu ostatnich 3 lat sprawdzeniu przez audytorów zewnętrznych i uzyskał pozytywną opinię w tym zakresie (np.: posiada certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z normą ISO/IEC 27001 w pełnym zakresie)?

TAK/NIE

1.1. Wymagania do pkt 1

- a) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia **kopii certyfikatu**, o którym mowa w pytaniu pkt 3.
- b) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 1 lub 2 przy jednoczesnej negatywnej odpowiedzi na pytanie pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia obowiązujących w organizacji odpowiednio: **kodeksu postępowania** lub **zasad ochrony danych osobowych** (np. polityki bezpieczeństwa informacji).

W przypadku negatywnych odpowiedzi na pytania zawarte w pkt 1 – 3 należy odpowiedzieć na pytania zawarte w kolejnych punktach.

2. STRUKTURA OCHRONY DANYCH, DOŚWIADCZENIE

- 1) Czy Podmiot zewnętrzny posiada doświadczenie w świadczeniu usług polegających na zarządzaniu zbiorami danych osobowych w imieniu innego podmiotu (pełnił rolę podmiotu przetwarzającego)?

TAK*/NIE

* Jeśli TAK, to proszę wskazać dla ilu podmiotów była taka usługa świadczona i przez jaki okres (łącznie, np.: 5 podmiotów, 8 lat):.....

- 2) Czy w trakcie świadczenia usług, o których mowa w pytaniu zawartym w pkt 1 doszło do naruszenia ochrony danych osobowych w zakresie powierzonych danych z winy podmiotu przetwarzającego?

TAK/NIE/NIE DOTYCZY

- 3) Czy Podmiot zewnętrzny wyznaczył w strukturach wewnętrznych Inspektora Ochrony Danych lub osobę/komórkę odpowiedzialną za nadzór nad ochroną danych osobowych? (właściwie zaznaczyć)

TAK – Inspektor Ochrony Danych (IOD)	
TAK – osoba (inna niż IOD)/ komórka odpowiedzialna za ochronę danych osobowych	
NIE	

- 4) Czy Podmiot zewnętrzny opracował i wdrożył metodykę oraz procedury zarządzania ryzykiem związanym z bezpieczeństwem informacji w tym metodykę oraz procedury przeprowadzania oceny skutków dla ochrony danych?

TAK/NIE

- 5) Czy Podmiot zewnętrzny prowadzi rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO?

TAK/NIE

- 6) Czy Podmiot zewnętrzny prowadzi rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO?

TAK/NIE

- 7) Czy Podmiot zewnętrzny przeprowadza regularne (co najmniej raz w roku) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?

TAK/NIE

- 8) Czy Podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, określonych w art. 15 - 22 RODO?

TAK/NIE

3. ZASADY OCHRONY DANYCH

3.1. DOSTĘP DO DANYCH

- 1) Czy Podmiot zewnętrzny zapewnia, aby każdy nowozatrudniony pracownik przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami o ochronie danych osobowych, w tym wewnętrznymi?

TAK/NIE

- 2) Czy podmiot przetwarzający prowadzi cykliczne szkolenia doskonalące dla swojego personelu lub podejmuje inne działania mające na celu podnoszenie świadomości pracowników i uaktualnianie wiedzy z zakresu ochrony danych osobowych?

TAK/NIE

- 3) Czy osoby wykonujące operacje na danych osobowych otrzymały stosowne upoważnienia do przetwarzania danych, spełniające wymogi przepisu art. 29 RODO?

TAK/NIE

- 4) Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania ich w tajemnicy/poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy? Czy zostało to udokumentowane?

TAK (bez dokumentacji)	
TAK – udokumentowane	
NIE	

- 5) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury nadawania uprawnień do systemów informatycznych przetwarzających dane osobowe, z zachowaniem zasad „wiedzy koniecznej”?

TAK/NIE

- 6) Czy Podmiot zewnętrzny prowadzi cykliczne przeglądy nadanych uprawnień?

TAK/NIE

- 7) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury bezzwłocznego odbierania uprawnień do systemów informatycznych przetwarzających dane osobowe, w stosunku do osób, dla których ustala celowość dostępu?

TAK/NIE

3.2. FIZYCZNY DOSTĘP DO OBSZARÓW PRZETWARZANIA

- 1) Czy Podmiot zewnętrzny stosuje środki kontroli dostępu fizycznego do budynku/budynków ograniczające dostęp tylko dla autoryzowanego personelu?

TAK/NIE

- 2) Czy Podmiot przetwarzający posiada odpowiednio wyposażone i zabezpieczone pomieszczenia umożliwiające bezpieczne przetwarzanie danych osobowych?

TAK/NIE

- 3) Czy Podmiot zewnętrzny zapewnia odpowiedni nadzór nad osobami niebędącymi jego pracownikami, a przebywającymi w jego siedzibie, także mających dostęp po godzinach pracy (personel sprzątający, personel ochrony fizycznej)?

TAK/NIE

- 4) Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?

TAK/NIE

3.3. OCHRONA DOMYŚLNA (PRIVACY BY DEFAULT)

- 1) Czy każdy pracownik otrzymuje unikalny identyfikator do systemów informatycznych?

TAK/NIE

- 2) w systemach informatycznych Podmiotu zewnętrznego zapewniono wymuszanie na użytkownikach stosowania haseł o odpowiedniej sile (kombinacja liter, cyfr i znaków specjalnych, min. 8 znakowe), także ich okresowej zmiany oraz zmian w razie zaistniałej potrzeby?

TAK/NIE

- 3) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego ekranu” polegającą na automatycznym wygaszaniu ekranu i blokowaniu systemu, po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła?

TAK/NIE

- 4) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego biurka” polegającą na obowiązku chowania dokumentów zawierających dane osobowe do zamykanych szaf na koniec dnia pracy?

TAK/NIE

- 5) Czy w systemach informatycznych Podmiotu zewnętrznego wykorzystywane jest jedynie oprogramowanie autoryzowane przez Kierownictwo Podmiotu zewnętrznego?

TAK/NIE

- 6) Czy w systemach informatycznych Podmiotu zewnętrznego są wdrożone zabezpieczenia wykrywające lub zapobiegające użyciu nieautoryzowanego oprogramowania?

TAK/NIE

- 7) Czy systemy informatyczne Podmiotu zewnętrznego są objęte rzeczywistą ochroną przed szkodliwym oprogramowaniem (zainstalowane i regularnie uaktualniane oprogramowanie antymalwerowe na wszystkich urządzeniach wykorzystywanych do przetwarzania danych, w tym telefonach komórkowych)?

TAK/NIE

- 8) Czy Podmiot zewnętrzny posiada wdrożony proces zarządzania podatnościami technicznymi, mający na celu redukcję podatności, które mogą być wykorzystane przez szkodliwe oprogramowanie lub umożliwić atak hackerski?

TAK/NIE

- 9) Czy posiadane przez Podmiot zewnętrzny sieci komputerowe, zarówno przewodowe jak i bezprzewodowe, poprzez odpowiednią konfigurację urządzeń i systemów, umożliwiają blokowanie podejrzanego transmisji danych?

TAK/NIE

- 10) Czy urządzenia mobilne (laptopy, tablety, telefony komórkowe, itp.) wykorzystywane do przetwarzania danych osobowych, którymi Podmiot zewnętrzny dysponuje, są szyfrowane?

TAK/NIE

- 11) Czy jest stosowane szyfrowanie komunikacji pomiędzy systemami Podmiotu zewnętrznego?

TAK/NIE

- 12) Czy Podmiot zewnętrzny posiada wdrożone procedury bezpiecznego zbywania sprzętu, uwzględniające całkowite usuwanie danych z nośników informacji?

TAK/NIE

- 13) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania incydentami związanymi z bezpieczeństwem informacji?

TAK/NIE

- 14) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania ciągłością działania?

TAK/NIE

3.4. OCHRONA NA ETAPIE PROJEKTOWANIA (PRIVACY BY DESIGN)

- 1) Czy posiadane przez Podmiot zewnętrzny środowiska produkcyjne, testowe oraz deweloperskie są niezależne, odseparowane od siebie, przynajmniej na poziomie VLAN-ów?

TAK/NIE

- 2) Czy Podmiot zewnętrzny dokonuje dla każdego projektu (dotyczącego wytworzenia nowego oprogramowania, jak również zmiany istniejącego) szacowania ryzyka pod kątem bezpieczeństwa informacji?

TAK/NIE

- 3) Czy Podmiot zewnętrzny wdrożył i stosuje procedury odbioru systemów przed uruchomieniem na środowisku produkcyjnym, z uwzględnieniem aspektów bezpieczeństwa informacji?

TAK/NIE

3.5. Wymagania do pkt 2 i 3

Podmiot zewnętrzny zobowiązany jest do przedłożenia stosownych zasad, procedur, o których mowa w pkt 2 i 3.

4. WERYFIKACJA ZASAD OCHRONY DANYCH

- 1) W przypadku udzielenia odpowiedzi negatywnej na jakiegokolwiek pytanie zawarte w pkt 2 oraz 3, czy Podmiot zewnętrzny wyraża gotowość do bezzwłocznego wdrożenia brakujących zasad?

TAK/NIE

- 2) Czy Podmiot zewnętrzny wyraża zgodę na ewentualną weryfikację w siedzibie Podmiotu zewnętrznego, opisanych powyżej zasad ochrony danych osobowych (sposób przeprowadzenia przez ARiMR audytu będzie uzgadniany indywidualnie)?

TAK/NIE

OŚWIADCZENIE

Działając w imieniu Podmiotu Przetwarzającego potwierdzam zgodność przedstawionych powyżej informacji pod rygorem odpowiedzialności prawnej, w tym odpowiedzialności wynikającej z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE. L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

.....

Data i podpis osoby upoważnionej