Załącznik nr 4 do SWZ stanowiący Załącznik nr 3
do projektowanych postanowień umownych (BOR08.2619.3.2025.DP)

POTWIERDZENIE WYKONANIA ŚWIADCZEŃ W RAMACH PRAWA OPCJI ZAKUPU

ZA MIESIĄC …….. / …… ROKU

W OPOLSKIM ODDZIALE REGIONALNYM / BIURZE POWIATOWYM W ……. *

Umowa nr …/OR08/2025/2619 z dnia ……. roku

Tabela nr 2 - Potwierdzenie wykonania świadczenia w zakresie interwencji /ochrony doraźnej (pkt 2.5 i 2.6 załącznika nr 2 do SWZ) w ramach prawa opcji zakupu)**		
ILOŚĆ WYKONANYCH ROBOCZOGODZIN INTERWENCJI /OCHRONY DORAŹNEJ 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 ppkt 1)-2) załącznika nr 2 do SWZ] w ramach prawa opcji zakupu)**		
ILOŚĆ WYKONANYCH ROBOCZOGODZIN W ROZLICZANYM MIESIĄCU	**ROZLICZANY MIESIĄC**	**ZAMAWIAJĄCY*****
Ilość roboczogodzin, w tym rozpoczętych: …….	Miesiąc ……rok …….	
Tabela nr 2 - Potwierdzenie wykonania świadczenia w zakresie dodania elementów systemów [pkt.2.4 ppkt 3) załącznika nr 2 do SWZ] w ramach prawa opcji zakupu)**		
ILOŚĆ WYKONANYCH ROBOCZOGODZIN W ROZLICZANYM MIESIĄCU	**ROZLICZANY MIESIĄC**	**ZAMAWIAJĄCY*****
Ilość roboczogodzin, w tym rozpoczętych: …….	Miesiąc ……rok …….	

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.

Załącznik nr 7 do SWZ stanowiący Załącznik nr 4
do projektowanych postanowień umownych (BOR08.2619.3.2025.DP)

ZGŁOSZENIE POTRZEBY WYKONANIA CZYNNOŚCI W RAMACH PRAWA OPCJI ZAKUPU

UMOWA NR …/OR08/2025/2619 Z DNIA …… R.

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/dodania elementów systemów w obrębie budynków dotychczas podlegających ochronie lub w nowej lokalizacji *:

Termin wykonania / czas reakcji*:

Miejsce wykonania:

* Niepotrzebne skreślić

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

Załącznik nr 9 do SWZ, stanowiący Załącznik nr 6
do projektowanych postanowień umownych (BOR08.2619.3.2025.DP)

Książka odbiorów świadczeń jednorazowych w ramach czynności: ochrony doraźnej, przyjazdu grupy interwencyjnej/ przeniesienia instalacji monitoringu do innego budynku/ dodania elementów systemów (*) w Oddziale Regionalnym …….. / Biurze Powiatowym ……. (*) do umowy nr …/OR08/2025/2619 z dnia …… r.

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:
……
……

…….
(Podpis osoby upoważnionej przez Zamawiającego)

…….
(Podpis osoby upoważnionej przez Wykonawcę)

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 samodzielne kod,
- ✓ uzbroić lokalny system alarmowy z pominięciem linii.

3. Załączenie i wyłączanie 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 wyłączania 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 indentyfikacyjnych:
- ✓ 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.

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. **…….. – Pan …….**

Zamawiający: **Wykonawca:**

Załącznik nr 12 do SWZ, stanowiący Załącznik nr 9
do projektowanych postanowień umownych
(BOR08.2619.3.2025.DP)

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:
Przegląd 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			
Przegląd techniczny i konserwacja systemu kontroli dostępu (SKD)				
1	sprawdzenie prawidłowości działania elektro zaczepów i elektrozawór 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			
Przegląd 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:	**Wykonawca:**
(data i czytelny podpis przedstawiciela Zamawiającego)	(data i czytelny podpis przedstawiciela Wykonawcy)

Załącznik nr 13 do SWZ, stanowiący Załącznik nr 10
do projektowanych postanowień umownych
(BOR08.2619.3.2025.DP)

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					

Załącznik nr 14 do SWZ, stanowiący Załącznik nr 11
do projektowanych postanowień umownych
(BOR08.2619.3.2025.DP)

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

Załącznik nr 15 do SWZ, stanowiący Załącznik nr 12
do projektowanych postanowień umownych
(BOR08.2619.3.2025.DP)

Zgłoszenie potrzeby przeniesienia instalacji monitoringu do innego budynku / dodania elementów systemów w obrębie budynków dotychczas podlegających ochronie lub w nowej lokalizacji wraz z włączeniem ich do systemu* :

na podstawie § 4 ust. 4 umowy nr …/OR08/2025/2619

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 / DODANIA*	
MIEJSCE DEMONTAŻU INSTALACJI*:	
MIEJSCE INSTALACJI*:	
TERMIN REALIZACJI ZLECENIA	
UWAGI:	

DATA, PIECZĄTKA I PODPIS OSOBY ZGŁASZAJĄCEJ

* niepotrzebne skreślić

Załącznik nr 16 do SWZ, stanowiący Załącznik nr 13
do projektowanych postanowień umownych
(BOR08.2619.3.2025.DP)

*(Wzór umowy do stosowania w przypadku powierzenia przetwarzania danych osobowych ARiMR poprzez przekazanie Wykonawcy danych na nośnikach papierowych lub informatycznych).***

Załącznik nr …….
(do Umowy nr …… z dnia ……..).

Umowa powierzenia przetwarzania danych osobowych
zawarta w dniu …….. w Warszawie
(dalej zwana także – „Umową Powierzenia").

pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, 00-175 Warszawa, REGON nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną w dalszej części umowy **„Zamawiającym" lub „Administratorem"**, reprezentowaną przez:

……...
a
……...

z siedzibą w ……. przy ul. ……., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy……., (…) Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem ……, NIP (…), REGON (...), posiadającą kapitał zakładowy w kwocie …….. zł, wpłacony w całości/…….. zamieszkałą/ym ……legitymującą/ym się……., prowadzącą/ym działalność gospodarczą pod nazwą ……, na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, z miejscem prowadzenia działalności gospodarczej w ……..……, REGON……, zarejestrowanym podatnikiem podatku od towarów i usług, NIP……., zwaną/ym dalej **„Wykonawcą",** reprezentowanym(ą) przez:

……...

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

§ 1
Powierzenie przetwarzania danych osobowych.

W celu wykonania Umowy nr ……. z dnia ……..... (dalej zwana także – „Umową") zawartej pomiędzy wyżej wymienionymi Stronami, Zamawiający powierza Wykonawcy w trybie art. 28 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) zwanego również „Rozporządzenie" lub „ogólne rozporządzenie o ochronie danych", przetwarzanie danych osobowych znajdujących się w zbiorach: Zamawiającego, a Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.

1. Wykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ogólnego rozporządzenia o ochronie danych i chroniło prawa osób, których te dane dotyczą. Wykonawca zobowiązuje się do przekazania Administratorowi - celem spełnienia wymogu rozliczalności - niezbędnych informacji i dokumentów lub innych dowodów potwierdzających realizację obowiązku, o którym mowa w zdaniu pierwszym.
2. Na podstawie Umowy powierzenia przetwarzania danych osobowych Strony określają jej przedmiot w następujący sposób:
   1) Zamawiający powierza Wykonawcy przetwarzanie danych osobowych w zakresie:
      a) charakter przetwarzania: forma elektroniczna (e-mail), forma papierowa, sposób ręczny i ciągły;
      b) kategoria osób, których dane dotyczą: pracownicy ARiMR;
      c) rodzaj danych osobowych: dane zwykłe: imię i nazwisko, numer telefonu;
   2) 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. Dane osobowe będą przekazane Wykonawcy przez Zamawiającego w następujący sposób: wielokrotnie, nośniki papierowe oraz za pomocą poczty elektronicznej.
4. Dane osobowe zostaną przekazane przez Zamawiającego po dostarczeniu mu przez Wykonawcę wykazu obszarów przetwarzania, przez który należy rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, w których powierzone dane będą przetwarzane. Wykaz obszarów przetwarzania będzie aktualizowany przez Wykonawcę, który w terminie 3 dni po każdej zmianie obszarów przetwarzania

powierzonych danych jest obowiązany dostarczyć Zamawiającemu nowy wykaz obszarów ich przetwarzania.

5. Strony ustalają, że odwołanie przez Wykonawcę umocowania udzielonego pełnomocnikowi, o którym mowa w ust. 4 dokonywane będzie na piśmie. O każdorazowym odwołaniu wskazanego powyżej upoważnienia Wykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego w formie pisemnej.
6. Wykonawca zobowiązuje się przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego. W przypadku, gdy obowiązek przetwarzania danych osobowych przez Wykonawcę wynika z obowiązujących przepisów prawa unijnego lub krajowego, Wykonawca informuje Administratora na piśmie lub drogą elektroniczną, na adresy wskazane w § 7 ust. 4 Umowy Powierzenia – przed rozpoczęciem przetwarzania – o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
7. Wykonawca zobowiązuje się niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie, o którym mowa w ust. 7 stanowi naruszenie ogólnego rozporządzenia o ochronie danych lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. Informacja ta powinna zawierać wskazanie przepisu prawa, który w ocenie Wykonawcy został naruszony i uzasadnienie oraz powinna być przekazana na piśmie lub drogą elektroniczną, na adres Administratora wskazany w § 7 ust. 4 Umowy Powierzenia.

§ 2
Zasady przetwarzania powierzonych danych osobowych.

1. Zamawiający jest administratorem danych osobowych w rozumieniu przepisów ogólnego rozporządzenia o ochronie danych.
2. Stosownie do przepisów ogólnego rozporządzenia o ochronie danych, Zamawiający powierza, a Wykonawca przyjmuje do przetwarzania dane osobowe wyłącznie w celu i zakresie niezbędnym do wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
3. Wykonawca nie będzie korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody Administratora. W przypadku pisemnej zgody Wykonawca poinformuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
4. Jeżeli do wykonania Umowy Wykonawca korzystać będzie z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają - na mocy Umowy dalszego powierzenia - te same obowiązki ochrony danych, jakie zostały określone w Umowie i Umowie powierzenia zawartych między Administratorem a Wykonawcą, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.
5. Wykonawca w umowie zawartej z innym podmiotem przetwarzającym zapewni, że podmiot ten nie będzie korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody Administratora.
6. Wykonawca w umowie zawartej z innym podmiotem przetwarzającym zapewni Administratorowi prawa określone w § 4 Umowy powierzenia.

7. Jeżeli inny podmiot przetwarzający, któremu zostały dalej powierzone dane nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Wykonawcy.
8. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową powierzenia, ogólnym rozporządzeniem o ochronie danych oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
9. Wykonawca zobowiązuje się wykonać wszelkie czynności i zobowiązania wynikające z Umowy Powierzenia i ogólnego rozporządzenia o ochronie danych z najwyższą starannością.
10. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Zamawiającego za przetwarzanie powierzonych danych osobowych, Wykonawca zobowiązuje się niezwłocznie zawiadomić o tych zagrożeniach Zamawiającego i podjąć wszelkie działania niezbędne dla usunięcia tych zagrożeń oraz natychmiast zawiadomić Zamawiającego o podjętych działaniach.
11. Wykonawca zobowiązuje się niezwłocznie, ale nie później niż w ciągu 3 dni roboczych (rozumianych jako dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy) do informowania Administratora o jakimkolwiek postępowaniu (w tym sądowym lub administracyjnym), którego przedmiot stanowi przetwarzanie powierzonych danych osobowych, o jakiejkolwiek decyzji administracyjnej lub rozstrzygnięciu odnoszącym się do przetwarzania tych danych, skierowanym do Wykonawcy, a także o wszelkich zaplanowanych lub prowadzonych kontrolach i inspekcjach u Wykonawcy, dotyczących przetwarzania powierzonych danych.
12. W przypadku wszczęcia przeciwko Zamawiającemu przez osobę trzecią jakiegokolwiek postępowania (w szczególności administracyjnego lub sądowego) opartego na twierdzeniu, że przetwarzanie powierzonych danych osobowych nastąpiło z naruszeniem przepisów Rozporządzenia, przepisów prawa krajowego wprowadzonych na mocy Rozporządzenia oraz innych przepisów prawa powszechnie obowiązującego, chroniących prawa osób, których dane dotyczą, Wykonawca zobowiązuje się na żądanie Zamawiającego do udzielenia Zamawiającemu wszelkich informacji i wyjaśnień oraz przekazania Zamawiającemu wszelkich dokumentów wymaganych przez Zamawiającego, potrzebnych mu do wzięcia udziału w tym postępowaniu. Wykonawca niniejszym zobowiązuje się do zapewnienia Zamawiającemu na swój koszt ochrony sądowej oraz do poniesienia konsekwencji zapadłego wyroku sądowego.
13. Wykonawca zobowiązuje się do udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczynianie się do nich.
14. Wykonawca oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy – EOG). Wykonawca oświadcza również, że nie korzysta z podwykonawców, którzy przekazują dane poza EOG.

§ 3
Zabezpieczenie powierzonych danych osobowych.

1. Wykonawca oświadcza, że będzie przetwarzał powierzone dane osobowe przy użyciu urządzeń i systemów informatycznych zapewniających odpowiedni poziom bezpieczeństwa przetwarzania, o którym mowa w art. 32 ogólnego rozporządzenia o ochronie danych, odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których powierzone dane dotyczą.
2. Wykonawca zobowiązuje się spełnić warunki, w tym podjąć środki zabezpieczające powierzone dane osobowe, o których mowa w art. 32 ogólnego rozporządzenia o ochronie danych. W szczególności Wykonawca zobowiązuje się do:
   1) zapewnienia kontroli nad prawidłowością przetwarzania powierzonych danych osobowych,
   2) zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia powierzonych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przypadkową lub niezgodną z prawem modyfikacją, utratą, zniszczeniem lub uszkodzeniem,
   3) dopuszczenia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania powierzonych danych osobowych wyłącznie osób, których dostęp do danych osobowych jest niezbędny dla realizacji Umowy i posiadających wydane przez niego upoważnienie,
   4) prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania powierzonych danych osobowych,
   5) 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,
   6) niewykorzystywania powierzonych danych osobowych dla celów innych niż wykonywanie Umowy, o której mowa w §1 ust. 1 Umowy Powierzenia,
   7) uwzględniając charakter przetwarzania, pomagania 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,
   8) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagania Administratorowi wywiązać się z obowiązków określonych w art. 32-36 ogólnego rozporządzenia o ochronie danych,
   9) w razie stwierdzenia naruszenia ochrony danych osobowych, zawiadomienia Zamawiającego o takim naruszeniu niezwłocznie (na piśmie i drogą elektroniczną, na adresy wskazane w §7 ust. 4 Umowy Powierzenia), lecz nie później niż w ciągu 12 godzin od jego wykrycia. 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,

10) prowadzenia w formie pisemnej (w tym elektronicznej) rejestru wszystkich kategorii czynności przetwarzania, dokonywanych w imieniu Zamawiającego.

§ 4
Nadzór nad wykonywaniem Umowy Powierzenia.

1. Zamawiający jest uprawniony w każdym czasie do przeprowadzania audytów sposobu wykonywania Umowy Powierzenia przez Wykonawcę, w tym sprawdzania czy środki techniczne i organizacyjne zabezpieczające przetwarzanie powierzonych danych, zastosowane przez Wykonawcę, odpowiadają ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Ponadto Zamawiający ma prawo dokonać weryfikacji, czy Wykonawca przetwarzając powierzone dane osobowe przestrzega przepisów ogólnego rozporządzenia o ochronie danych 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.
2. W celu wykonania audytu upoważnieni pracownicy Zamawiającego mają prawo:
   1) wstępu do obszarów przetwarzania powierzonych danych osobowych (m.in. pomieszczeń) i przeprowadzania czynności audytowych,
   2) pozyskania informacji o sposobie przetwarzania powierzonych danych,
   3) żądania od Wykonawcy udostępnienia dokumentów, złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
   4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych Wykonawcy służących do przetwarzania powierzonych danych osobowych,
3. Z czynności audytowych przeprowadzający audyt pracownicy Zamawiającego sporządzają protokół w dwóch egzemplarzach – podpisany przez przedstawicieli obu Stron – z których jeden egzemplarz doręcza się Wykonawcy.
4. Wykonawca zapewnia możliwość niezwłocznego przeprowadzenia czynności audytowych przez Zamawiającego w każdym z obszarów przetwarzania powierzonych danych osobowych. Osoby uprawnione do przeprowadzenia audytu 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 audytu.
5. W przypadku ujawnienia okoliczności uznanych przez Zamawiającego za nieprawidłowości w zakresie wykonywania Umowy Powierzenia lub ogólnego rozporządzenia o ochronie danych, Wykonawca zobowiązuje się do ich usunięcia w wyznaczonym przez Zamawiającego terminie. 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 ……..zł (słownie: ……. złotych) za każdy przypadek stwierdzonej i nieusuniętej w terminie nieprawidłowości.

6. Jeżeli nieprawidłowości wskazane w ust. 5 zostaną ponownie ujawnione, Zamawiający może naliczyć Wykonawcy karę umowną w wysokości wskazanej w ust. 5 bez wyznaczania terminu do usunięcia tych nieprawidłowości.
7. W przypadku naliczenia kary umownej, Zamawiający może według własnego wyboru:
   1) potrącać karę umowną z łącznego wynagrodzenia za wykonanie Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
   2) skorzystać z zabezpieczenia należytego wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
   3) wezwać Wykonawcę do zapłaty kary umownej w terminie 14 dni od dnia doręczenia pisemnego wezwania do jej zapłaty.

§ 5
Przetwarzanie powierzonych danych osobowych
po wygaśnięciu Umowy Powierzenia.

1. Umowa Powierzenia wygasa z upływem 14 dni od dnia wykonania, rozwiązania, wygaśnięcia, unieważnienia lub odstąpienia od Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
2. W przypadku wystąpienia okoliczności, o której mowa w ust. 1, Wykonawca zobowiązuje się niezwłocznie, nie później jednak niż w terminie 14 dni od dnia wystąpienia tej okoliczności, trwale usunąć wszelkie powierzone mu na podstawie Umowy Powierzenia dane osobowe oraz wszelkie ich istniejące kopie, w tym skutecznie usunąć te dane z nośników elektronicznych pozostających w jego dyspozycji lub zwrócić dane, chyba że prawo Unii lub prawo państwa członkowskiego nakazują dalej przechowywanie danych osobowych. Zamawiający celem zweryfikowania wykonania przez Wykonawcę zobowiązań wskazanych w zdaniu pierwszym niniejszego ustępu uprawniony jest do przeprowadzenia audytu na zasadach wskazanych w §4 ust. 1-4 Umowy Powierzenia.
3. Powierzenie przetwarzania danych osobowych trwa do upływu terminu wskazanego w ust. 1.
4. Celem usunięcia wątpliwości Strony ustalają, że pomimo wygaśnięcia Umowy Powierzenia zachowują moc obowiązującą wszelkie postanowienia nakładające lub mogące nałożyć na Wykonawcę jakiekolwiek zobowiązanie względem Zamawiającego, po terminie wygaśnięcia Umowy Powierzenia, w tym m.in. postanowienia §2 ust. 8, §5 ust. 2 i §5 ust. 5 Umowy Powierzenia.
5. W przypadku niewykonania przez Wykonawcę zobowiązania wynikającego z treści §5 ust. 2 Umowy Powierzenia Zamawiający uprawniony jest do naliczenia Wykonawcy kary umownej w wysokości ……. zł (słownie: …… złotych). W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia §4 ust. 7 Umowy Powierzenia.
6. W przypadku naruszenia przez Wykonawcę zobowiązania, o którym mowa w § 3 ust. 2 pkt 5, Zamawiający uprawniony jest do naliczenia Wykonawcy kary umownej w wysokości …… zł (słownie: zł) za każdy przypadek naruszenia. W przypadku naliczenia kary umownej wskazanej w zdaniu pierwszym niniejszego ustępu stosuje się odpowiednio postanowienia § 4 ust. 7 Umowy Powierzenia.
7. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy Powierzenia powstanie szkoda przewyższająca zastrzeżoną karę umowną, o której mowa

w § 4 ust. 5 i § 5 ust. 5 Umowy 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.

§ 6
Wykonywanie Umowy Powierzenia.

1. Wynagrodzenie z tytułu wykonania Umowy Powierzenia zawarte jest w wynagrodzeniu przewidzianym dla Wykonawcy w § ……. ust. …….. Umowy.
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 wystąpienia zdarzenia, o którym mowa w § 2 ust. 8 niniejszej Umowy Powierzenia.
4. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Wykonawca:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas audytu 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.

§ 7
Postanowienia końcowe.

1. Wszelkie zmiany Umowy Powierzenia dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych Umową Powierzenia mają zastosowanie w szczególności przepisy Kodeksu cywilnego oraz przepisy ogólnego rozporządzenia o ochronie danych.
3. Sądem właściwym dla rozstrzygania sporów powstałych w związku z zawarciem lub wykonywaniem Umowy Powierzenia jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Wszelka korespondencja w sprawach związanych z Umową Powierzenia będzie kierowana do:
   a) Administratora na następujące dane kontaktowe: adres: Wrocławska 170G, 45-835 Opole, tel. 77 401 84 22, e-mail opolski@arimr.gov.pl;
   b) Wykonawcy na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…).
5. Dane przedstawicieli Stron:
   a) Administratora w kontaktach z Wykonawcą w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: Dagmara Walerianczyk, Robert Sadowski;
   b) Wykonawcę w kontaktach z Administratorem w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…).

6. Zmiana adresów i danych osób wskazanych w ust. 4 i 5 nie stanowi zmiany Umowy Powierzenia. O każdej zmianie powyższych danych Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.
7. Umowa Powierzenia wchodzi w życie z dniem jej podpisania przez Strony.
8. Umowę Powierzenia sporządzono w czterech jednobrzmiących egzemplarzach – trzy dla Zamawiającego i jeden dla Wykonawcy.

ZAMAWIAJĄCY WYKONAWCA

……. ……

Klauzula informacyjna

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator 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, wskazanych w pkt 1.
3. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c) RODO oraz na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz. U. z 2024 r., poz. 1320) dalej „*ustawa Pzp"* w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego znak: BOR08.2619.3.2025.DP na usługę ochrony całodobowej obiektów w Opolskim Oddziale Regionalnym i Biurach Powiatowych ARiMR oraz jego rozstrzygnięcia; w przypadku udzielenia zamówienia publicznego Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. b RODO w celu zawarcia oraz wykonania umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania, w oparciu o art. 18 oraz art. 74 ust. 2 ustawy Pzp,
   2) organy kontrolne,
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające dane osobowe w imieniu Administratora na mocy zawartych innych umów, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały okres obowiązywania umowy w sprawie zamówienia publicznego. W przypadku zawarcia i realizacji umowy okres przechowywania obejmuje również okres niezbędny do zabezpieczenia ewentualnych roszczeń wynikających z umowy, chyba, że przepisy szczegółowe stanowią inaczej. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat na potrzeby archiwizacji.
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach *ustawy Pzp* w związku z art. 6 ust. 1 lit. c RODO związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości udzielenia Pani/Panu zamówienia publicznego przez ARiMR
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. Posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **; żądanie ograniczenia przetwarzania nie znajduje zastosowania do czasu zakończenia niniejszego postępowania;

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

9. Nie przysługuje Pani/Panu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO, prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Miejscowość ..... dnia ..... r.

Zapoznałam/em się i przyjmuję powyższe do wiadomości

.....
(pieczęć i podpis osoby/ób uprawnionej/ych do składania oświadczeń woli w imieniu Wykonawcy lub czytelny podpis w przypadku osób fizycznych)

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy/zamówienia.
** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

Znak sprawy: BOR08.2619.3.2025.DP

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 pomiotów 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? (właściwe 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 teleinformatycznych 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 teleinformatycznych przetwarzających dane osobowe, w stosunku do osób, dla których ustała 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 teleinformatycznych?

TAK/NIE

2) w systemach teleinformatycznych 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 teleinformatycznych Podmiotu zewnętrznego wykorzystywane jest jedynie oprogramowanie autoryzowane przez Kierownictwo Podmiotu zewnętrznego?

TAK/NIE

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

TAK/NIE

7) Czy systemy teleinformatyczne 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 redukowanie 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 podejrzanej 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 jakiekolwiek 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 04.03.2021, str. 35).

…….

Data i podpis osoby upoważnionej