25 lat
Agencja Restrukturyzacji
i Modernizacji Rolnictwa
Al. Jana Pawła II 70, 00-175 Warszawa

**Adres korespondencyjny:**

**Agencja Restrukturyzacji i Modernizacji Rolnictwa**
**ul. Poleczki 33**
**02-822 Warszawa**

**numer referencyjny sprawy: DPiZP.2610.4.2020**

# Specyfikacja Istotnych Warunków Zamówienia

**(dalej: SIWZ)**

w postępowaniu o udzielenie zamówienia publicznego
o wartości powyżej 139 000 €
prowadzonym w trybie przetargu nieograniczonego

**na**:
**„Zakup usługi wsparcia Systemu Contact Center"**

wszczętym na podstawie ustawy z dnia 29 stycznia 2004 r.
- Prawo zamówień publicznych (tj.: Dz. U. z 2019 r. poz. 1843)

**INFORMACJE OGÓLNE DOTYCZĄCE PROWADZONEGO POSTĘPOWANIA**

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w języku polskim. Komunikacja między Zamawiającym a Wykonawcami w niniejszym postępowaniu odbywa się przy użyciu środków komunikacji elektronicznej, tj. „Platformy Zakupowej" dostępnej pod adresem https://platformazakupowa.pl/pn/arimr (dalej: „Platforma Zakupowa").

2. Informacje i dokumenty związane z przedmiotowym postępowaniem zostały zamieszczone w zakładce „Postępowania". W celu zapoznania się z zamieszczonymi informacjami lub dokumentami należy przejść na formularz postępowania.

3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu o udzielenie zamówienia publicznego:

   1) Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nie posiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się" w kolejnym kroku należy wybrać „Załóż konto", następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy, nieobowiązkowo nr telefonu.

   2) Złożenie oferty oraz oświadczenia, o którym mowa w art. 25a z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (tj.: Dz. U. z 2019 r. poz. 1843; dalej: „ustawa"), w tym Jednolitego Europejskiego Dokumentu Zamówienia składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.

   3) Wykonawca składa ofertę, która w przypadku prawidłowego złożenia oferty zostaje automatycznie zaszyfrowana przez system. Nie jest możliwe zapoznanie się z treścią złożonej oferty przed upływem terminu otwarcia ofert.

   4) Podpisanie dokumentów w formie skompresowanej poprzez opatrzenie całego pliku jednym podpisem kwalifikowanym jest równoznaczne z poświadczaniem za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów. Dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym. Podpisanie skompresowanego pliku, w którym umieszczono dokument w formie oryginału nie stanowi podpisania tego dokumentu.

4. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia Prezesa Rady Ministrów w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępnienia i przechowywania dokumentów elektronicznych (Dz. U. z 2017 r. poz. 1320; dalej: „Rozporządzenie w sprawie środków komunikacji"), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie Zakupowej, tj.:

   1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,

   2) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,

   3) zainstalowana dowolna przeglądarka internetowa; w przypadku Internet Explorer minimalnie wersja 10.0.,

   4) włączona obsługa JavaScript,

   5) zainstalowany program Adobe Acrobat Reader, lub inny obsługujący format plików .pdf.

5. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 75 MB. Zalecany format: .pdf.

6. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat kodowania i czasu odbioru danych, tj.:

   1) Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany nie jest widoczny dla Zamawiającego, gdyż jest w systemie jako zaszyfrowany. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez system, co następuje po terminie otwarcia ofert,

   2) Oznaczenie czasu odbioru danych przez Platformę stanowi przypiętą do oferty elektronicznej datę oraz dokładny czas (hh:mm:ss), znajdujące się w kolumnie dotyczącej danej oferty, w sekcji - "Data złożenia oferty".

7. Zamawiający, zgodnie z § 4 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalny format kwalifikowanego podpisu elektronicznego jako:

   1) dokumenty w formacie .pdf zaleca się podpisywać formatem PAdES;

   2) dopuszcza się podpisanie dokumentów w formacie innym niż .pdf, wtedy zaleca się użyć formatu XAdES.

8. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr w zakładce „Regulamin" oraz uznaje go za wiążący.

9. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści siwz, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr.

10. Korzystanie z Platformy Zakupowej jest bezpłatne. W celu ułatwienia Wykonawcom korzystania z Platformy Zakupowej operator platformy uruchomił Centrum Wsparcia Klienta, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: **cwk@platformazakupowa.pl**

**Rozdział I. Przedmiot zamówienia.**

**I.1. Opis przedmiotu zamówienia.**

1. Kod Wspólnego Słownika Zamówień (CPV).
   Główny kod: 72267000-4 [Usługi w zakresie konserwacji i napraw oprogramowania].
2. Przedmiotem zamówienia jest:
   2.1. zapewnienie Agencji Restrukturyzacji i Modernizacji Rolnictwa (dalej: „ARiMR" lub „Zamawiający") możliwości korzystania z Usługi Asysty Technicznej dla Oprogramowania wskazanego w Załączniku nr 1 do wzoru Umowy, zgodnie z ogólnymi warunkami Producenta oraz postanowieniami wzoru Umowy wraz z załącznikami stanowiącym Załącznik nr 5 do SIWZ
   2.2. świadczenie Usługi Wsparcia obejmującej:
      2.2.1. zakres wskazany w Załączniku nr 2 do wzoru Umowy stanowiącym Załącznik nr 5 do SIWZ,
      2.2.2. przeprowadzenie Warsztatów dla maksymalnie 10 wskazanych pracowników Zamawiającego na warunkach i zasadach określonych we wzorze Umowy wraz z załącznikami stanowiącym Załącznik nr 5 do SIWZ,
      2.2.3. zapewnienie 500 godzin konsultacji administracyjnych oraz związanych z działaniem Oprogramowania i Systemu Contact Center w języku polskim, w tym do zlecania prac programistycznych, w szczególności polegających na modyfikacji Systemu Contact Center lub jego dokumentacji w zakresie dedykowanych potrzeb Zamawiającego związanych z korzystaniem z Systemu Contact Center. Konsultacje oraz prace programistyczne realizowane będą w Lokalizacji Zamawiającego lub zdalnie drogą elektroniczną (e-mail, skype) lub telefoniczną, przez programistów lub administratorów Wykonawcy legitymujących się doświadczeniem z zakresu posługiwania się Oprogramowaniem.

   2.3. Usługa Asysty Technicznej i Usługa Wsparcia są odrębnymi usługami o określonym zakresie i realnej wartości, co powinno znaleźć odzwierciedlenie w ofercie zgodnie z Formularzem Ofertowym. W związku z powyższym wartość Konsultacji realizowanych w ramach Usługi Wsparcia obejmująca swym zakresem ppkt 2.2.3. wskazany w Rozdziale I.1 pkt 2 musi stanowić maksymalnie 20% ceny oferty.

3. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych we wzorze Umowy wraz z załącznikami stanowiącym Załącznik nr 5 do SIWZ.

**I.2. Opis części zamówienia.**

Zamawiający nie dopuszcza składania przez Wykonawcę ofert częściowych w rozumieniu art. 2 pkt 6) ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zm.; dalej: „ustawa").

**I.3. Powierzenie Podwykonawcy wykonania części zamówienia.**

1. Zamawiający dopuszcza powierzenie Podwykonawcom wykonania części zamówienia.
2. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć Podwykonawcy oraz do podania firm Podwykonawców.

**I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia.**

1. Zamawiający przewiduje udzielenie zamówień, o których mowa w art. 67 ust. 1 pkt 6) ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu art. 2 pkt 7) ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej na podstawie art. 99 ustawy, jak również nie przewiduje przeprowadzenia aukcji elektronicznej.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5. Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

**Rozdział II. Termin wykonania zamówienia.**

1. Zamawiający wymaga, aby zamówienie było realizowane przez okres 24 miesięcy począwszy od dnia zawarcia Umowy.

**Rozdział III. Warunki udziału w postępowaniu oraz podstawy wykluczenia.**

1. O zamówienie mogą ubiegać się Wykonawcy, którzy:
   1.1. Nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy oraz art. 24 ust. 5 pkt 1 ustawy;
   1.2. Spełniają warunki udziału w postępowaniu w zakresie zdolności zawodowej. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
      1.2.1. wykonał, w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie **minimum 2 (dwie) usługi obejmujące swoim zakresem zapewnienie wsparcia technicznego dla oprogramowania aplikacyjnego, o wartości brutto każdej z nich nie mniejszej niż 400 000,00 zł (słownie: czterysta tysięcy złotych 00/100).**).

   **UWAGA 1**
   Jeżeli wartość usługi wskazanej w wykazie jest podana w walucie innej niż PLN, Wykonawca zobowiązany jest, na potrzeby niniejszego postępowania, dokonać przeliczenia jej wartości na PLN wg średniego kursu NBP (www.nbp.pl tabela A – tabela kursów średnich walut obcych) z dnia zakończenia usługi o zakresie jak wyżej wraz z podaniem kursu oraz daty jego obowiązywania (zgodnie z tabelą A – tabela kursów średnich walut obcych) wg których dokonano przeliczenia; w przypadku usług nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej usługi.

   **UWAGA 2**
   W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:
   1) brak podstaw wykluczenia, o których mowa w pkt 1.1 musi spełniać każdy Wykonawca z osobna,
   2) warunki udziału w postępowaniu określone w pkt 1.2 musi spełniać co najmniej jeden Wykonawca lub wszyscy Wykonawcy łącznie.

2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdziale IV niniejszej SIWZ. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.

3. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 25a ust. 1 ustawy, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
4. Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
5. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę:
   5.1. na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy,
   5.2. na podstawie art. 24 ust. 5 pkt 1 ustawy, tj. Wykonawcę w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2019 r. poz. 243 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2019 r. poz. 498 ze zm.),
6. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania.
7. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 24aa ustawy, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza (na podstawie kryteriów oceny ofert określonych w SIWZ) nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

**Rozdział IV. Zawartość ofert, wykaz oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu.**

W zakresie nieuregulowanym postanowieniami SIWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r. poz. 1126 ze zm. dalej: „Rozporządzenie w sprawie rodzajów dokumentów").

**IV.1. Zawartość ofert.**

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ) **za pośrednictwem Platformy Zakupowej**.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
   2.1. Pełnomocnictwo do podpisania oferty pod rygorem nieważności w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez osobę/y upoważnione do reprezentacji wskazane we właściwym rejestrze, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym. Zamawiający dopuszcza złożenie elektronicznej kopii pełnomocnictwa poświadczonej przez notariusza.
   2.2. Dowód wniesienia wadium - dokument wadium, oryginał gwarancji/poręczenia, jeżeli Wykonawca wnosi wadium w innej formie niż pieniądz opatrzone kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). W przypadku wniesienia wadium w innej formie niż pieniądz, powinno ono obowiązywać przez cały okres związania ofertą.
   2.3. Zobowiązanie podmiotu trzeciego lub inny dokument potwierdzający, że Wykonawca będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym przez osobę upoważnioną do reprezentacji wskazane we właściwym rejestrze. Zapisy Rozdziału IV.5 SIWZ stosuje się odpowiednio.
   2.4. Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (dalej: „JEDZ") sporządzone zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE. Dokument JEDZ należy złożyć pod rygorem nieważności w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym.

**IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia.**

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
   1.1. Zamawiający udostępnia Wykonawcom plik, w formacie xml, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 6 do SIWZ.
   1.2. Zamawiający informuje, że pod adresem: **https://espd.uzp.gov.pl** Urząd Zamówień Publicznych udostępnił nieodpłatne narzędzie umożliwiające Zamawiającym i Wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ (JEDZ/ESPD) w wersji elektronicznej (eESPD).
2. Oświadczenia podmiotów składających ofertę wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ muszą mieć formę dokumentu w postaci elektronicznej podpisanego kwalifikowanym podpisem elektronicznym przez każdy z tych podmiotów w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy.
3. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
4. Dokument elektroniczny JEDZ należy złożyć w formacie .pdf).

5. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 26 ust. 3 ustawy; W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.
6. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu składa także oświadczenia JEDZ, o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ, dotyczące tych podmiotów.

**IV.3. Oświadczenia lub dokumenty, potwierdzające spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.**

1. Wykonawca obowiązany jest w terminie **3 dni od dnia zamieszczenia na stronie internetowej** Zamawiającego (Platformie Zakupowej) - www.platformazakupowa.pl/pn/arimr **informacji**, o których mowa w art. 86 ust. 5 ustawy, **do przekazania Zamawiającemu oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy**. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Wzór oświadczenia stanowi Załącznik nr 3 do SIWZ.
2. Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności w poniższym zakresie:
   2.1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
      2.1.1. informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy,
      2.1.2. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy,
      2.1.3. oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności,
      2.1.4. oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
   2.2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:
      2.2.1. wykazu usług wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. Wzór oświadczenia stanowi Załącznik nr 4 do SIWZ.

3. Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w Rozdziale IV.3 pkt 2.1.1 SIWZ, składa na Platformie Zakupowej, podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności dokument, o którym mowa w Rozdziale IV.4 pkt 1.1 SIWZ, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Postanowienia Rozdziału IV.4 pkt 2 SIWZ zdanie pierwsze stosuje się.
4. Jeżeli treść informacji przekazanych przez Wykonawcę w JEDZ odpowiada zakresowi informacji, których Zamawiający wymaga poprzez żądanie dokumentów, w szczególności o których mowa w pkt 2.2, Zamawiający zastrzega sobie prawo do odstąpienia od żądania tych dokumentów od Wykonawcy. W takim przypadku dowodem spełniania przez Wykonawcę warunków udziału w postępowaniu oraz braku podstaw wykluczenia są odpowiednie informacje przekazane przez Wykonawcę lub odpowiednio przez podmioty, na których zdolnościach lub sytuacji Wykonawca polega na zasadach określonych w art. 22a ustawy, w JEDZ.

**IV.4. Dokumenty składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej.**

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w Rozdziale:
   1.1. IV.3 pkt 2.1.1 SIWZ – składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy,

1.2. IV.3 pkt 2.1.2 SIWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

1.2.1. nie otwarto jego likwidacji ani nie ogłoszono upadłości.

2. Dokumenty, o których mowa w pkt 1.1 oraz 1.2.1, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 1, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Postanowienia pkt 2 stosuje się.

**IV.5. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów.**

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

2. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

3. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda złożenia przez Wykonawcę dokumentów, które określają w szczególności:

3.1. zakres dostępnych Wykonawcy zasobów innego podmiotu,

3.2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,

3.3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego,

3.4. czy podmiot, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.

4. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdziale IV.3 ppkt 2.1.1 -2.1.4 SIWZ.

**IV.6. Klauzule informacyjne w zakresie danych osobowych.**

1. W związku z treścią 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 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.), dalej: „RODO" Zamawiający informuje, że:

1.1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II nr 70, 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.

1.2. 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 1.1.

1.3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.

1.4. Odbiorcami Pani/Pana danych osobowych mogą być:

1.4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy,

1.4.2. organy kontrolne,

1.4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2019 poz. 1429),

1.4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.

1.5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 97 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.

1.6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.

1.7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

1.8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

**Rozdział V. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.**

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem formy elektronicznej. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.
2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPiZP.2610.4.2020**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem formy elektronicznej za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji istotnych warunków zamówienia (SIWZ). Wniosek należy przesłać za pośrednictwem Platformy Zakupowej. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Treść pytań (bez ujawnienia źródła) wraz z wyjaśnieniami bądź informacje o dokonaniu modyfikacji SIWZ, Zamawiający przekaże Wykonawcom za pośrednictwem Platformy Zakupowej.
5. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego po upływie terminu jego składania, o którym mowa w pkt 4 lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
6. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SIWZ.
7. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
8. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
   8.1. Pani Katarzyna Mazur, tel. +48 22 595-00-63 w godz. 9.00 – 15.00.
   8.2. Pan Henryk Żywno, tel.: +48 22 595-00-67 w godz. 9.00 – 15.00.

**Rozdział VI. Wymagania dotyczące wadium.**

1. Wykonawca zobowiązany jest wnieść wadium w wysokości: **10 000,00 zł** (słownie: dziesięć tysięcy złotych zero groszy).
2. Wadium może być wniesione w:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tj.: Dz. U. z 2019 r., poz. 310 ze zm.).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku - 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: „wadium w postępowaniu na **„**Zakup usługi wsparcia Systemu Contact Center**"**.
4. W przypadku wnoszenia wadium w innej formie niż pieniądz Wykonawca wnosi w formie elektronicznej poprzez wczytanie na Platformie Zakupowej oryginału dokumentu wadialnego tj. opatrzonego kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny i nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadium musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 46 ust. 4a i ust. 5 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i ust. 5 ustawy.
7. Oferta Wykonawcy, który nie wniesie wadium lub wniesie je w sposób nieprawidłowy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

**Rozdział VII. Termin związania ofertą.**

Wykonawcy pozostają związani złożoną ofertą przez 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

**Rozdział VIII Opis sposobu przygotowywania ofert.**

**VIII.1. Przygotowanie ofert.**

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ). Oferta oraz dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym (każdy plik osobno podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności).
2. Treść złożonej oferty musi odpowiadać treści niniejszej SIWZ. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w postaci elektronicznej pod rygorem nieważności i podpisana kwalifikowanym podpisem elektronicznym wyłącznie za pośrednictwem Platformy Zakupowej.
3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.

4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 86 ust. 4 ustawy, tj. nazwa (firma) Wykonawcy, adres Wykonawcy, informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji, warunków płatności zawarte w ofercie.

   Uwaga: Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010), które Wykonawca pragnie zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.
6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
   6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,
   6.2. każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi udokumentować, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 oraz art. 24 ust. 5 pkt 1 ustawy, a także złożyć informację lub listę, o której mowa w Rozdziale IV.3 pkt 1 SIWZ,
   6.3. zgodnie z art. 23 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub do reprezentowania ich w postępowaniu oraz zawarcia umowy o udzielenie przedmiotowego zamówienia publicznego,
   6.4. wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem,
   6.5. przed podpisaniem umowy przedłożą pełnomocnictwo do zawarcia umowy w sprawie zamówienia publicznego, jeżeli pełnomocnictwo takie nie zostało dołączone do oferty.

**VIII.2. Forma dokumentów składanych w postępowaniu.**

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2019 r. poz. 162).
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. Dokumenty lub oświadczenia, o których mowa w Rozporządzeniu w sprawie rodzajów dokumentów, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem.
4. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.
5. Poświadczenia za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, o której mowa w pkt 4 następuje przy użyciu kwalifikowanego podpisu elektronicznego.
6. Ilekroć w SIWZ, a także w załącznikach do SIWZ występuje wymóg podpisywania dokumentów lub oświadczeń lub też potwierdzania dokumentów lub oświadczeń za zgodność z oryginałem, należy przez to rozumieć że oświadczenia i dokumenty te powinny być opatrzone kwalifikowanym podpisem elektronicznym osoby (osób) uprawnionej (uprawnionych) do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega na podstawie pełnomocnictwa.

**Rozdział IX. Miejsce oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty.**

**IX.1. Miejsce oraz termin składania ofert i otwarcia ofert.**

1. Ofertę pod rygorem nieważności należy złożyć w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej https: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **15.05.2020 r. o godzinie 11:00** Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone po upływie terminu przewidzianego na wniesienie odwołania, po uprzednim zawiadomieniu Wykonawcy o fakcie złożenia oferty po terminie.
3. Otwarcie ofert odbędzie się w dniu **15.05.2020 r. o godzinie 11:15** w biurze Zamawiającego, pod adresem ul. Poleczki 33, 02-822 Warszawa.
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SIWZ.

**IX.2. Warunki zmiany i wycofania złożonej oferty.**

1. Wykonawca posiadający konto na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić lub wycofać ofertę.
2. Wykonawca nie posiadający konta na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić ofertę. Wykonawca niezalogowany nie może samodzielnie wycofać oferty. W celu wycofania oferty należy skontaktować się z Centrum Wsparcia Klienta uruchomione przez Operatorem Platformy Zakupowej, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mail: cwk@platformazakupowa.pl.
3. Na Platformie Zakupowej w zakładce „Instrukcje dla Wykonawców" opisana jest szczegółowa procedura zmiany i wycofania oferty.
4. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty (załączników).

**Rozdział X. Opis sposobu obliczenia ceny.**

1. Wykonawca zobowiązany jest do wyliczenia i podania cen jednostkowych, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SIWZ.
2. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdziału XIV pkt 4 niniejszej SIWZ.
3. Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
6. Usługa Asysty Technicznej i Usługa Wsparcia są odrębnymi usługami o określonym zakresie i realnej wartości, co powinno znaleźć odzwierciedlenie w ofercie zgodnie z Formularzem Ofertowym. W związku z powyższym wartość Konsultacji realizowanych w ramach Usługi Wsparcia obejmująca swym zakresem ppkt 2.2.3. wskazany w Rozdziale I.1 pkt 2 musi stanowić maksymalnie 20% ceny oferty.

**Rozdział XI. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert.**

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:

**1)** **<u>kryterium cena</u> ($P_c$) – waga 60%,** wg poniższego wzoru

$$P_C = \frac{C_{min.}}{C_b} \text{ x 60 pkt}$$

<u>gdzie:</u>
**$P_C$** **–** ilość punktów oferty badanej w kryterium cena
***$C_{min.}$*** **–** cena najniższa spośród ważnych ofert
***$C_b$*** **–** cena oferty badanej

**2)** **kryterium „dodatkowe godziny konsultacji",** o których mowa w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ **($P_k$) – waga 20 %, wg poniższej zasady:**

| Lp. | **Dodatkowe godziny konsultacji,** o których mowa w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ | Ilość punktów |
|---|---|---|
| 1 | 0 godzin dodatkowych | 0 pkt |
| 2 | 20 godzin dodatkowych | 5 pkt |
| 3 | 50 godzin dodatkowych | 10 pkt |
| 4 | 100 godzin dodatkowych | 20 pkt |

***<u>Uwagi:</u>***
*a) Zamawiający może przyznać maksymalnie 20 pkt.*
*b) Ilość dodatkowych godzin konsultacji - wskazana przez Wykonawcę w Formularzu Ofertowym, zostanie wpisana w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ.*
*c) W przypadku braku wskazania ilości dodatkowych godzin konsultacji w Formularzu Ofertowym, Zamawiający uzna, że Wykonawca zaoferował 0 (zero) dodatkowych godzin konsultacji*
*d) Jeżeli Wykonawca zaoferuje ilość dodatkowych godzin konsultacji powyżej 100 godzin, Zamawiający wpisze tą ilość do postanowień Umowy (§ 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 100 godzin dodatkowych konsultacji i Wykonawca otrzyma maksymalną ilość punktów tj. 20 pkt.*

**3) kryterium „Czas realizacji (Awaria)”,** o którym mowa w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ **($P_A$) – waga 10 %, wg poniższej zasady:**

| Lp. | **„Czas realizacji (Awaria)”** | Ilość punktów |
|---|---|---|
| 1 | 4 godziny | 0 pkt |
| 2 | 3 godziny | 5 pkt |
| 3 | 2 godziny | 10 pkt |

**Uwagi:**

*a) Maksymalny „Czas realizacji (Awaria)”, o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *wynosi 4 godziny.*

*b) Jeżeli Wykonawca zaoferuje „Czas realizacji (Awaria)”, o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *dłuższy niż 4 godziny – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*

*c) Jeżeli Wykonawca zaoferuje „Czas realizacji (Awaria)”, o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *krótszy niż 2 godziny – Zamawiający wpisze tą ilość do postanowień Umowy (*pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej *Załącznik nr 5 do SIWZ) natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 2 godziny i Wykonawca otrzyma maksymalną ilość punktów tj. 10 pkt.*

*d) W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin „Czas realizacji (Awaria)”, o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *tj.: 4 godziny.*

**4) kryterium „Czas realizacji (Usterka)”**, o którym mowa w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ **($P_U$) – waga 10 %, wg poniższej zasady:**

| Lp. | **„Czas realizacji (Usterka)”** | Ilość punktów |
|---|---|---|
| 1 | 48 godzin | 0 pkt |
| 2 | 24 godziny | 2 pkt |
| 3 | 12 godzin | 5 pkt |
| 4 | 8 godzin | 10 pkt |

**Uwagi:**

*a) Maksymalny „Czas realizacji (Usterka)”, o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *wynosi 48 godzin.*

*b) Jeżeli Wykonawca zaoferuje „Czas realizacji (Usterka)”, o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *dłuższy niż 48 godzin – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*

*c) Jeżeli Wykonawca zaoferuje „Czas realizacji (Usterka)”, o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *krótszy niż 8 godzin – Zamawiający wpisze tą ilość do postanowień Umowy (*pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej *Załącznik nr 5 do SIWZ) natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 8 godzin i Wykonawca otrzyma maksymalną ilość punktów tj. 10 pkt.*

*d) W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin „Czas realizacji (Usterka)”, o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ, *tj.: 48 godzin.*

2. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów obliczoną z dokładnością do dwóch miejsc po przecinku wg wzoru:

$$P = P_c + P_k + P_A + P_U$$

gdzie:

**P** – ilość punktów oferty w łącznym kryterium oceny ofert,

**$P_c$** – ilość punktów oferty w kryterium „**cena”,**

**$P_k$** – ilość punktów oferty w kryterium **dodatkowe godziny konsultacji”,** o których mowa w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ,

**$P_A$** – ilość punktów oferty w kryterium **„Czas realizacji (Awaria)”,** o którym mowa w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ,

**$P_U$ –** ilość punktów oferty w kryterium **„Czas realizacji (Usterka)”**, o którym mowa w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ**.**

**Rozdział XII. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.**

1. Zamawiający powiadomi wybranego Wykonawcę o miejscu i terminie podpisania umowy.
2. Wykonawca będzie zobowiązany do niezwłocznego podania Zamawiającemu danych niezbędnych do sporządzenia umowy lub przekazania dokumentów, które okażą się konieczne do zawarcia umowy.

**Rozdział XIII.**

**Wymagania dotyczące zabezpieczenia należytego wykonania umowy.**

1. Zamawiający żąda od Wykonawcy z którym zostanie podpisana umowa wniesienia zabezpieczenia należytego wykonania umowy w wysokości **5 %** ceny całkowitej podanej w ofercie.
2. Zabezpieczenie należytego wykonania umowy może być wniesione w następujących formach:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
3. W przypadku wniesienia zabezpieczenia w formie pieniężnej Zamawiający przechowuje je na oprocentowanym rachunku bankowym.
4. Zabezpieczenie wnoszone w formie gwarancji bankowej, ubezpieczeniowej, poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, poręczenia udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, ma być wystawione przez bank, ubezpieczyciela lub poręczyciela. Bank, ubezpieczyciel, poręczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę zabezpieczenia, na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
5. W przypadku, gdy zabezpieczenie, o którym mowa w niniejszym Rozdziale SIWZ będzie wnoszone w formie innej niż pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentów.
6. Zabezpieczenia w innej formie niż pieniądz, Wykonawca złoży u Zamawiającego w Kancelarii Głównej, mieszczącej się w Warszawie przy ul. Poleczki 33, z adnotacją „dla Departamentu Informatyki".
7. Zabezpieczenie należytego wykonania umowy służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
8. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w terminach i na zasadach określonych we wzorze umowy.

**Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego.**

1. Zawarcie umowy nastąpi wg wzoru Umowy Zamawiającego, stanowiącego Załącznik nr 5 do niniejszej SIWZ.
2. Postanowienia ustalone we wzorze Umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.
4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego we wzorze Umowy wraz z załącznikami, stanowiącym Załącznik nr 5 do SIWZ.

**Rozdział XV. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia publicznego.**

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale VI ustawy.
2. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy.
3. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
5. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   6.1. 10 (dziesięciu) dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej, albo w terminie 15 (piętnastu) dni – jeżeli zostały przesłane w inny sposób;
   6.2. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia SIWZ na stronie internetowej – wobec treści ogłoszenia oraz wobec postanowień SIWZ;
   6.3. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia – wobec czynności innych niż określone w pkt 6.1 i 6.2 powyżej.
7. W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub postanowień SIWZ Zamawiający może przedłużyć termin składania ofert.
8. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

**Załączniki do SIWZ:**

1. Załącznik nr 1 wzór Formularza Ofertowego.
2. Załącznik nr 2 - wzór Oświadczenie o braku podstaw wykluczenia.
3. Załącznik nr 3 - wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej.
4. Załącznik nr 4 - wzór Oświadczenia – Wykaz usług (*warunek udziału w postępowaniu*)
5. Załącznik nr 5 – wzór Umowy wraz z załącznikami.
6. Załącznik nr 6 - ESPD – plik, w formacie xml, wygenerowany z narzędzia ESPD – do przygotowania Formularza Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ).

Zatwierdzam SIWZ wraz z załącznikami:

Signature Not Verified
Dokument podpisany przez Jolanta Joanna Piechocka; ARiMR
Data: 2020.04.09 07:47:58 CEST

Warszawa, …….

*p.o. Zastępcy Prezesa ARiMR*
*Jolanta Piechocka*
*podpis Zamawiającego*

**Załącznik nr 1 do SIWZ wzór Formularza Ofertowego**

**Formularz Ofertowy**
**DPiZP.2610.4.2020**

Ja(my) niżej podpisany(-i)

……

Działając w imieniu i na rzecz

……

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na **„Zakup usługi wsparcia Systemu Contact Center”**, zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

**Tabela nr 1 - Usług Asysty Technicznej dla Oprogramowania:**

| ***L.p.*** | **Przedmiot** Nazwa Oprogramowania/licencji (APN Number) | ***Ilość licencji*** | ***Cena netto za jeden okres rozliczeniowy (12 miesięcy) w którym świadczona będzie Usługa Asysty Technicznej dla ilości oprogramowania wskazanego w kol. c*** | ***Ilość okresów rozliczeniowych*** | ***Cena netto [zł]*** | ***Podatek VAT*** | | ***Cena brutto [zł]*** |
|---|---|---|---|---|---|---|---|---|
| | | | | | | ***%*** | ***[zł]*** | |
| *[a]* | *[b]* | *[c]* | *[d]* | *[e]* | *[f]=[d] x [e]* | *[g]* | *[h]=[f] x [g]* | *[i]=[f] + [h]* |
| 1. | Genesys CIM Platform (3GP21278ACAA) | 35 | | **2** | | | | |
| 2. | Genesys CPD/ASM (3GP21282ACAA) | 30 | | **2** | | | | |
| 3. | Genesys Callback (3GP21929ACAA) | 30 | | **2** | | | | |
| 4. | Genesys Chat (3GP80855ACAA) | 30 | | **2** | | | | |
| 5. | Genesys Co-browse (3GP21944ACAA) | 30 | | **2** | | | | |
| 6. | Genesys Customer Experience Insights (3GP84586ACAA) | 35 | | **2** | | | | |
| 7. | Genesys E-mail (3GP21059ACAA) | 35 | | **2** | | | | |
| 8. | Genesys Info Mart (3GP21747ACAA) | 35 | | **2** | | | | |
| 9. | Genesys Outbound Voice (3GP08809ACAA) | 30 | | **2** | | | | |
| 10. | Genesys SIP Interaction (3GP09017ACAA) | 35 | | **2** | | | | |
| 11. | Genesys SMS (3GP21886ACAA) | 30 | | **2** | | | | |
| 12. | Genesys Social Engagement Pkg (3GP21219ACAA) | 5 | | **2** | | | | |
| 13. | Genesys Softphone (3GP21208ACAA) | 35 | | **2** | | | | |
| 14. | Genesys Workforce Management (3GP20738ACAA) | 35 | | **2** | | | | |
| 15. | Interaction Recording - Voice Edition (3GP20166ACAA) | 15 | | **2** | | | | |
| 16. | Proactive Contact - E-mail/SMS (3GP08822ACAA) | 1 | | **2** | | | | |
| 17. | SIP Qualification & Parking (3GP21844ACAA) | 18 | | **2** | | | | |
| 18. | Workspace (3GP20364ACAA) | 35 | | **2** | | | | |
| 19. | intelligent Workload Distribution & JMS Adapter (3GP21286ACAA) | 5 | | **2** | | | | |
| 20. | RecViewer Voice recording (Custom) | 35 | | **2** | | | | |
| **Razem:** | | | | **2** | | **X** | | |

## Usługa Wsparcia na które składa się:

**Tabela nr 2**

| Lp. | Przedmiot zamówienia | Ilość miesięcy | Cena netto za 1 miesiąc (zł) | Podatek VAT | | Cena brutto za 1 miesiąc (zł) | Cena netto (zł | Cena brutto (zł) |
|---|---|---|---|---|---|---|---|---|
| | | | | % | zł | | | |
| *[a]* | *[b]* | *[c]* | *[d]* | *[e]* | *[f] = [d] x [e]* | *[g] = [d] + [f]* | *[h] = [c] x [d]* | *[i] = [c] x [g]* |
| 1. | Usługa Wsparcia obejmująca:<br>a) zakres wskazany w Załączniku nr 2 do wzoru Umowy,<br>b) Warsztaty o których mowa w § 5 wzoru Umowy | **24*** | | | | | | |

**Tabela nr 3**

| Lp. | Przedmiot zamówienia | Ilość godzin | Cena netto za 1 godzinę konsultacji (zł) | Podatek VAT | | Cena brutto za 1 godzinę konsultacji (zł) | Cena netto (zł | Cena brutto* (zł) |
|---|---|---|---|---|---|---|---|---|
| | | | | % | zł | | | |
| *[a]* | *[b]* | *[c]* | *[d]* | *[e]* | *[f] = [d] x [e]* | *[g] = [d] + [f]* | *[h] = [c] x [d]* | *[i] = [c] x [g]* |
| 1. | Konsultacje, o których mowa w § 4 ust. 5 pkt 1) wzoru Umowy | **500**** | | | | | | |

***Uwaga!***

** Cena Konsultacji, o których mowa w Tabeli 3 musi stanowić maksymalnie 20% ceny oferty.*

*** Podana przez Zamawiającego w Tabeli nr 3 „Ilość godzin" – stanowi wartość wyłącznie szacunkową służącą celowi porównania ofert. Faktyczna ilość wykorzystania „Ilości godzin" będzie wynikać z rzeczywistych potrzeb Zamawiającego. Łączne wynagrodzenie Wykonawcy z tytułu wykonania Umowy wyniesie nie więcej niż Łączna cena oferty wynikająca z Tabeli nr 4 Formularza Ofertowego i podana poniżej.*

**Tabela nr 4 Łączna cena oferty**

| *L.p.* | Przedmiot | Cena netto w zł | Podatek VAT | | Cena brutto w zł |
|---|---|---|---|---|---|
| | | | % | zł | |
| *[a]* | *[b]* | *[c]* | *[d]* | [e] = [c] x [d] | *[f] = [c] + [e]* |
| 1. | **Usługa Asysty Technicznej dla Oprogramowania wg Tabeli nr 1** (Cena netto z Tabeli nr 1 – Razem kol. f) | | | | |
| 2. | **Usługa Wsparcia – wg Tabeli nr 2** (Cena netto z Tabeli nr 2 – kol. h) | | | | |
| 3. | **Usługa Wsparcia – wg Tabeli nr 3** (Cena netto z Tabeli nr 3 – kol. h) | | | | |
| **Łączna cena oferty w zł:** | | | **X** | | |

**Cena ofertowa netto słownie: ……**

**Cena ofertowa brutto słownie: ……**

**Oświadczamy, że:**

1. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdziale II SIWZ oraz wzorze Umowy.
2. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
3. Zapoznaliśmy się z treścią SIWZ (w tym ze wzorem Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
4. **W ramach zaoferowanej ceny zrealizujemy ……. dodatkowych godzin konsultacji, o których mowa w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ.**

   *Uwaga:*

   a) *Ilość dodatkowych godzin konsultacji - wskazana przez Wykonawcę w Formularzu Ofertowym, zostanie wpisana w § 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ.*
   b) *W przypadku braku wskazania ilości dodatkowych godzin konsultacji w Formularzu Ofertowym, Zamawiający uzna, że Wykonawca zaoferował 0 (zero) dodatkowych godzin konsultacji*
   c) *Jeżeli Wykonawca zaoferuje ilość dodatkowych godzin konsultacji powyżej 100 godzin, Zamawiający wpisze tą ilość do postanowień Umowy (§ 4 ust. 5 pkt 2 wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ) natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 100 godzin dodatkowych konsultacji i Wykonawca otrzyma maksymalną ilość punktów tj. 20 pkt.*

5. **Czas realizacji (Awaria),** o którym mowa w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ**, wyniesie …… godzin.**

   *Uwaga!*

   a) *Maksymalny „Czas realizacji (Awaria)", o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, wynosi 4 godziny.*
   b) *Jeżeli Wykonawca zaoferuje „Czas realizacji (Awaria)", o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, dłuższy niż 4 godziny – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*
   c) *Jeżeli Wykonawca zaoferuje „Czas realizacji (Awaria)", o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, krótszy niż 2 godziny – Zamawiający wpisze tą ilość do postanowień Umowy (*pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej *Załącznik nr 5 do SIWZ) natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 2 godziny i Wykonawca otrzyma maksymalną ilość punktów tj. 10 pkt.*
   d) *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin „Czas realizacji (Awaria)", o którym mowa* w pkt 5 lit. b) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, tj.: 4 godziny.*

6. **Czas realizacji (Usterka)**, o którym mowa w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ **wyniesie …… godzin.**

   **Uwagi:**

   a) *Maksymalny „Czas realizacji (Usterka)", o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, wynosi 48 godzin.*
   b) *Jeżeli Wykonawca zaoferuje „Czas realizacji (Usterka)", o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, dłuższy niż 48 godzin – oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*
   c) *Jeżeli Wykonawca zaoferuje „Czas realizacji (Usterka)", o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, krótszy niż 8 godzin – Zamawiający wpisze tą ilość do postanowień Umowy (*pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej *Załącznik nr 5 do SIWZ) natomiast do celów oceny ofert uzna, iż Wykonawca zaoferował 8 godzin i Wykonawca otrzyma maksymalną ilość punktów tj. 10 pkt.*
   d) *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin „Czas realizacji (Usterka)", o którym mowa* w pkt 5 lit. c) Załącznika nr 2 do wzoru Umowy stanowiącej Załącznik nr 5 do SIWZ*, tj.: 48 godzin.*

7. Uważamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.
8. Wadium w wysokości **10 000,00 zł** (słownie: dziesięć tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
9. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr ……prowadzony w banku …….
10. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **5%** ceny całkowitej podanej w ofercie.
11. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
12. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz firmę Podwykonawcy):

    a) ……
    ……*

    * *w* przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*

    ***UWAGA:***

    *Zamawiający przypomina, że powyższy punkt Formularza Ofertowego należy wypełnić w każdym przypadku, jeśli Wykonawca zamierza powierzyć podwykonawcom wykonanie części zamówienia, a także mając na uwadze treść art. 22a ust. 4 ustawy cyt.:*
    *„W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują roboty budowlane lub usługi, do realizacji których te zdolności są wymagane."*

    **Udział podmiotu trzeciego w realizacji zamówienia w odniesieniu do warunków winien mieć charakter podwykonawstwa, w związku z czym wypełnieniu podlega pkt 12 Formularza Ofertowego.**

13. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres: ……
    Dane kontaktowe: imię i nazwisko ……, nr tel. …….., adres e-mail: ……..
14. Dokumenty wymienione od strony …… do strony …… stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione pozostałym uczestnikom postępowania.

***UWAGA****:*

*Zamawiający przypomina, że stosownie do art. 8 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.*

15. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)* wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**

** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2).*

*** w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

16. Jednocześnie zgodnie z treścią art. 91 ust. 3a ustawy oświadczam, że wybór przedmiotowej oferty:
    a) **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego*)
    b) **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług*)

---

*(należy wskazać: nazwę (rodzaj) towarów/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz wartość bez kwoty podatku od towarów i usług)*

*) Niepotrzebne skreślić. W przypadku nie skreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: *„należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług”* – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

17. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr_____ do nr _____.

*Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).*

**Załącznik nr 2 do SIWZ wzór Oświadczenia o braku podstaw wykluczenia**

Dane Wykonawcy
(nazwa; adres)

**Oświadczenie o braku podstaw wykluczenia**

**DPIZP.2610.4.2020**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Zakup usługi wsparcia Systemu Contact Center"** oświadczam(-y), że:

1) nie wydano wobec nas prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne***** / wydano wobec nas prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, wobec czego składamy niżej wymienione dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności*****:
   a) ……..,
   b) ……..,
   c) ……..,
   d) ……..,
2) nie wydano orzeczenia wobec nas tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne.

***** UWAGA: niepotrzebne skreślić

**Załącznik nr 3 do SIWZ wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej**

Dane Wykonawcy
(nazwa; adres)

**Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej**

**DPIZP.2610.4.2020**

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Zakup usługi wsparcia Systemu Contact Center"**

**1)** Oświadczamy, że nie należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r., poz. 369 ze zm.)* **z żadnym z Wykonawców, którzy złożyli ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego**.**

**2)** Oświadczamy, że należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r., poz. 369 ze zm.) * **z następującymi Wykonawcami, którzy złożyli ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego**:**

| Lp. | Nazwa podmiotu | Siedziba |
|---|---|---|
| | | |
| | | |

[*Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia*]

* UWAGA: niepotrzebne skreślić

**Załącznik nr 4 do SIWZ wzór Oświadczenia – Wykaz usług**

*[warunek udziału w postępowaniu]*

Dane Wykonawcy
(nazwa; adres)

**Oświadczenie – Wykaz usług**
**DPIZP.2610.4.2020**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Zakup usługi wsparcia Systemu Contact Center",** składamy wykaz usług wykonanych (wykonywanych) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełniania warunku udziału w postępowaniu , o którym mowa w Rozdziale III pkt.1.2.1 SIWZ:

| Lp. | Przedmiot wykonanych/wykonywanych usług (wg warunku udziału w postępowaniu: zamówienie polegające na zapewnieniu wsparcia technicznego dla oprogramowania aplikacyjnego) | Wartość brutto usługi w zł *(w przypadku gdy zakres usługi jest szerszy, należy podać wyłącznie wartość usługi odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu: co najmniej* **400 000,00 *zł brutto***) | Podmiot na rzecz którego wykonano usługę *(nazwa i adres)* | Daty wykonania | | Dowody | Informacje uzupełniające | |
|---|---|---|---|---|---|---|---|---|
| | | | | Od dd-mm-rrrr | Do dd-mm-rrrr | | Zasoby innego podmiotu | Nazwa innego podmiotu |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | *9* |
| 1 | | | | | | | | |
| 2 | | | | | | | | |

*Uwaga do kol.7:*

1. *Do wykazu należy dołączyć dowody potwierdzające, że powyższe usługi zostały wykonane lub są wykonywane należycie, tj.:*
   - *1.1. referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane należycie,*
   - *1.2. oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1;*
2. *Należy wpisać nazwę dowodu (dokumentu) potwierdzającego, że usługi zostały wykonane wykonywane należycie (podać numer strony w ofercie);*

*Uwaga do kol.8:*

1. *Zaznaczyć „TAK", tylko w przypadku gdy Wykonawca polega na zasobach innego podmiotu dla wykazania spełniania warunku udziału;*
2. *Dla wykazania spełniania warunku udziału w postępowaniu, opisanego w Rozdziale III pkt 1.2.1 SIWZ, Wykonawca może polegać, na zasadach określonych w art.22a ustawy. W tym celu Wykonawca składa dokumenty i oświadczenia zgodnie z* zasadami *określonymi w Rozdziale IV.5 SIWZ.*

**Załącznik nr 5 do SIWZ wzór Umowy**

**Wzór Umowy**

**UMOWA Nr_____/DI/2020/___**

zawarta w dniu ___ .___.2020 roku w Warszawie, pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie i adresem przy Al. Jana Pawła II nr 70, 00-175 Warszawa, (adres do korespondencji: ARiMR Departament Informatyki ul. Poleczki 33, 02-822 Warszawa), REGON 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, reprezentowaną przez:

…… – ……
…… – ……

zwaną dalej „Zamawiającym"

a
…….z siedzibą w ……..i adresem:……., wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla…… w ……., …… Wydział Gospodarczy Krajowego Rejestru Sądowego pod Nr KRS ……., o kapitale zakładowym w wysokości ……zł, REGON ……, zarejestrowanym podatnikiem podatku od towarów i usług, NIP …… reprezentowaną przez:……**/**

……zamieszkałą ……., legitymującą się ……, prowadzącą 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 ……, reprezentowaną przez:

……

zwaną dalej „Wykonawcą",

o następującej treści:

**§ 1.**

**Definicje**

W niniejszej umowie następujące wyrażenia i określenia będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z wielkiej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

1) **Aktualizacja** - Updates (zaktualizowanie), Upgrade (ulepszenie), Patches (poprawka) oraz wszelkie nowe wersje Oprogramowania i udoskonalenia do wersji bieżących Oprogramowania (nowe edycje, wydania uzupełniające, poprawki programistyczne) wraz z ich dokumentacją, wydane przez Producenta;
2) **Dni Robocze** – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy;
3) **Lokalizacje**– Centrala ARiMR, ul. Poleczki 33, Warszawa;
4) **Oprogramowanie** – oprogramowanie wykorzystywane do funkcjonowania Systemu CC, wskazane w Załączniku nr 1 do Umowy, do którego prawo do korzystania Zamawiający nabył na podstawie odrębnej Umowy dla którego będzie świadczona Usługa Asysty Technicznej w ramach Umowy;
5) **Producent**- firma Genesys Telecommunications Laboratories Inc. z siedzibą w Daly City w Kalifornii;
6) **Strony** – Zamawiający i Wykonawca wymienieni w komparycji Umowy;
7) **System CC**- system Contact Center umożliwiający komunikację klientów zewnętrznych lub wewnętrznych z ARiMR przez wiele kanałów komunikacji (tzw. Multichanel) do którego prawo Zamawiający nabył na podstawie odrębnej umowy, dla którego będzie świadczona Usługa Wsparcia w ramach Umowy;
8) **Umowa** – niniejsza umowa wraz z załącznikami, regulująca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
9) **Usługa Asysty Technicznej** – usługa polegająca na zapewnieniu Zamawiającemu wsparcia technicznego dla Oprogramowania w okresie wskazanym w § 2 ust. 1 pkt 1 Umowy, zgodnie z ogólnymi warunkami Producenta;

10) **Usługa Wsparcia** – usługa polegająca na świadczeniu serwisu technicznego dla Systemu CC przez wykwalifikowany personel tj. osobę/osoby z doświadczeniem, posiadające odpowiednie kwalifikacje merytoryczne i wiedzę na temat Oprogramowania i Systemu CC, w tym polegająca na świadczeniu konsultacji administracyjnych oraz prac programistycznych związanych z działaniem Oprogramowania i Systemu CC lub dostosowaniem Oprogramowania do potrzeb Zamawiającego, z której Zamawiający uprawniony będzie do korzystania zgodnie z warunkami Umowy (w tym zgodnie z załącznikiem nr 2) w okresie wskazanym w § 2 ust. 1 pkt 1 Umowy;

11) **Warsztaty** –zajęcia praktyczne dotyczące funkcjonalności Systemu CC, prowadzone przez Wykonawcę dla wskazanych pracowników Zamawiającego, zgodnie z zakresem tematycznym i warunkami określonymi w Umowie.

**§ 2.**

**Przedmiot Umowy i termin realizacji**

1. Przedmiotem Umowy jest:

   1) zapewnienie Zamawiającemu możliwości korzystania z Usługi Asysty Technicznej zgodnie z Umową oraz ogólnymi warunkami Producenta oraz świadczenie przez Wykonawcę na rzecz Zamawiającego Usługi Wsparcia na warunkach określonych w Umowie, przez okres 24 miesięcy od dnia zawarcia Umowy,

   2) przeprowadzenie Warsztatów dla maksymalnie 10 wskazanych pracowników Zamawiającego.

2. Zamawiający uprawniony jest w ramach Usługi Wsparcia do zamawiania konsultacji oraz prac programistycznych do wyczerpania łącznego limitu godzin wskazanych w § 4 ust. 5 Umowy, nie dłużej jednak niż do upływu terminu wskazanego w ust. 1 pkt 1.

**§ 3.**

**Wymagania dotyczące wykonania Umowy**

1. Wykonawca oświadcza, że posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu należytej staranności określonej w art. 355 § 2 Kodeksu Cywilnego, w tym jest uprawniony przez Producenta do świadczenia Usługi Wsparcia oraz do zapewnienia Usługi Asysty Technicznej zgodnie z Umową w tym do udzielania w imieniu Producenta licencji na Aktualizacje.

2. Wykonawca nie ma prawa, bez zgody Zamawiającego, do korzystania przy wykonywaniu Umowy w jakimkolwiek charakterze z osób zatrudnionych u Zamawiającego, pod rygorem odstąpienia od Umowy przez Zamawiającego (w terminie 15 dni od wystąpienia przesłanki uprawniającej do odstąpienia) oraz zapłaty kary umownej w wysokości określonej w § 9 ust. 1 Umowy wraz z prawem do żądania od Wykonawcy odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.

3. Wykonawca zobowiązany jest do:

   1) przestrzegania regulacji wewnętrznych Zamawiającego dotyczących bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych, w szczególności wskazanych w ust. 4;

   2) przestrzegania obowiązujących u Zamawiającego przepisów, w szczególności w zakresie ochrony informacji wrażliwych, w tym danych osobowych oraz innych informacji prawnie chronionych;

   3) nieujawniania osobom trzecim informacji uzyskanych w trakcie i po wykonywaniu Umowy bez zgody Zamawiającego.

4. Wykonawca zobowiązuje się do wykonania Umowy w sposób spełniający wymogi bezpieczeństwa informacji, których treść jest określona w poniższych załącznikach do Polityki bezpieczeństwa informacji w ARiMR stanowiącej załącznik do Zarządzenia Prezesa ARiMR 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Agencji Restrukturyzacji i Modernizacji Rolnictwa stanowiących załącznik nr 5 do Umowy:

   1) „Regulamin użytkownika" - załącznik nr 5;

   2) „Regulamin zarządzania incydentami” – załącznik nr 8;

   3) „Regulamin ochrony danych osobowych”- załącznik nr 14.

5. Wykonawca zobowiązuje się do przeszkolenia pracowników i osób trzecich, realizujących objęte Umową zadania, w zakresie zachowania zasad bezpieczeństwa informacji określonych w dokumentach stanowiących załącznik nr 5 do Umowy oraz zasad przetwarzania danych osobowych określonych w przepisach o ochronie danych osobowych.

6. Wykonawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów 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 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej także: „RODO”.

7. Wykonawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 6.
8. Wykonawca oświadcza, że zapoznał się z klauzulą informacyjną w zakresie przetwarzania danych osobowych, stanowiącą załącznik nr 6 do Umowy.
9. Wykonawca zobowiązuje się do złożenia oświadczenia o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane bezpośrednio lub pośrednio pozyskał w celu zawarcia oraz wykonania Umowy zgodnie z wzorem oświadczenia stanowiącym załącznik nr 7 do Umowy.

**§ 4**

**Zakres Usługi Wsparcia**

1. W ramach Usługi Wsparcia świadczonej przez Wykonawcę, Zamawiający będzie miał prawo do korzystania z konsultacji administracyjnych związanych z działaniem Oprogramowania i Systemu CC w języku polskim, w tym do zlecania prac programistycznych, w szczególności polegających na modyfikacji Systemu CC lub jego dokumentacji w zakresie dedykowanych potrzeb Zamawiającego związanych z korzystaniem z Systemu CC. Konsultacje oraz prace programistyczne realizowane będą w Lokalizacji Zamawiającego lub zdalnie drogą elektroniczną (e-mail, skype) lub telefoniczną, przez programistów lub administratorów Wykonawcy legitymujących się doświadczeniem z zakresu posługiwania się Oprogramowaniem, pod numerem telefonu: ……, e-mail: …….w Dniach Roboczych w godzinach 8:00- 15:00, z zastrzeżeniem, że Wykonawca zostanie poinformowany przez Zamawiającego o konieczności konsultacji/realizacji prac programistycznych w Lokalizacji Zamawiającego z wyprzedzeniem co najmniej 2 (dwóch) Dni Roboczych. Czasu związanego z dojazdem Wykonawcy do biura Zamawiającego nie wlicza się do limitu godzin, o którym mowa w ust 5.
2. Wykonawca zobowiązany jest potwierdzić przyjęcie zgłoszenia drogą elektroniczną na e mail _____niezwłocznie, jednak nie dłużej niż w ciągu 2 godzin od momentu jego otrzymania. Niepotwierdzenie zgłoszenia w powyższym terminie Zamawiający uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu poczty elektronicznej lub numerów telefonów wskazanych powyżej, Wykonawca zobowiązany jest niezwłocznie powiadomić na piśmie Zamawiającego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie pisemnego aneksu.
3. Konsultacje w ramach Usługi Wsparcia polegać będą w szczególności na udzielaniu Zamawiającemu asysty lub doradztwa przy:
   1) implementacji i automatyzacji procesów biznesowych u Zamawiającego;
   2) realizowanych przez Zamawiającego pracach programistycznych;
   3) konfiguracji Systemu CC i Oprogramowania.
4. Wykonawca zobowiązany jest do bieżącego rozwiązywania problemów zgłaszanych w trakcie konsultacji, nie później jednak niż w ciągu 7 godzin od zgłoszenia problemu przez Zamawiającego. Zgłoszenie potrzeby konsultacji złożone do Wykonawcy po godzinie 15:00 powinno zostać obsłużone do godziny 15:00 następnego Dnia Roboczego. Strony mogą uzgodnić inne terminy realizacji konsultacji, przy uwzględnieniu specyfiki zgłaszanego problemu. Terminy wykonania prac programistycznych zostaną uzgodnione każdorazowo przez Strony.
5. Wykonawca zapewni Zamawiającemu możliwość skorzystania z konsultacji w tym prac programistycznych w ramach Usługi Wsparcia do:
   1) 500 godzin, przez okres wskazany w § 2 ust 1. pkt 1 Umowy,
   2) dodatkowych …… godzin konsultacji (*zgodnie z deklaracją Wykonawcy złożoną w pkt 4 Formularza Ofertowego*) w okresie obowiązywania Umowy, przy czym Zamawiający zastrzega, że dodatkowe godziny konsultacji będą wykorzystane w pierwszej kolejności i bez dodatkowego wynagrodzenia.

   Łączna liczba konsultacji w tym prac programistycznych udzielonych/zrealizowanych w danym miesiącu świadczenia Usługi Wsparcia, po ich zsumowaniu, będzie zaokrąglona do pełnej godziny, zgodnie z zasadą że jeśli zsumowana wartość przekracza pełną godzinę powyżej 30 minut, jest zaokrąglana do kolejnej pełnej godziny.
6. Wykonawca zobowiązany będzie w całym okresie świadczenia Usługi Wsparcia do cyklicznego (co poniedziałek) informowania Zamawiającego o łącznej liczbie wykorzystanego przez pracowników Zamawiającego czasu konsultacji oraz czasu prac programistycznych, wraz z opisem wykonanych zadań w ramach zrealizowanych świadczeń.
7. Wykonanie przez Wykonawcę zobowiązań z tytułu Usługi Wsparcia w każdym miesiącu jej świadczenia zostanie potwierdzone przez upoważnionych przedstawicieli Stron Miesięcznym Protokołem Świadczenia Usług, którego wzór stanowi Załącznik nr 3 do Umowy. W protokole tym będzie odnotowany czas udzielonych konsultacji w tym świadczonych prac programistycznych jak również zostaną wskazane utwory wykonane na rzecz Zamawiającego w danym okresie rozliczeniowym.

**§ 5.**

**Warsztaty**

1. Wykonawca, w ramach wynagrodzenia za Usługę Wsparcia, zobowiązany będzie do przeprowadzenia Warsztatów dla maksymalnie 10 pracowników wskazanych przez Zamawiającego, w języku polskim, przy czym łączny czas Warsztatów nie przekroczy 25 godzin.
2. Warsztaty odbędą się w Lokalizacji Zamawiającego w terminach uzgodnionych przez Strony, w trakcie obowiązywania Umowy.
3. Warsztaty obejmą zakresem tematycznym zagadnienia funkcjonowania Systemu CC i jego konfiguracji. Agenda Warsztatów zostanie ustalona między Stronami.
4. Przeprowadzenie Warsztatów zostanie potwierdzone podpisaniem przez Zamawiającego bez zastrzeżeń Protokołu Przeprowadzenia Warsztatów, zgodnie z wzorem stanowiącym załącznik nr 4 do Umowy.
5. W przypadku jakichkolwiek zastrzeżeń merytorycznych co do sposobu i jakości prowadzonych Warsztatów, Zamawiający ma prawo żądać od Wykonawcy powtórzenia Warsztatów na koszt Wykonawcy, w terminie wyznaczonym przez Zamawiającego.

**§ 6.**

**Usługa Asysty Technicznej**

1. W ramach Usługi Asysty Technicznej zapewnionej przez Wykonawcę, Zamawiający będzie miał prawo do:
   1) otrzymywania Aktualizacji wraz z dokumentacją Aktualizacji (o ile dla danej Aktualizacji została przez Producenta wytworzona); Wykonawca na podstawie Umowy udziela Zamawiającemu licencji uprawniającej do nieograniczonego w czasie korzystania przez Zamawiającego z Aktualizacji wraz z dokumentacją Aktualizacji, zgodnie z ogólnymi warunkami licencyjnymi Producenta, na następujących zasadach:
      a) Wykonawca w ramach udzielonej licencji upoważnia Zamawiającego do trwałego lub czasowego zwielokrotnienia Aktualizacji w całości lub części jakimikolwiek środkami i w jakiejkolwiek formie, jak i zwielokrotniania również w zakresie, w którym jest to niezbędne dla wprowadzania do pamięci sprzętu Zamawiającego, wyświetlania, stosowania, przystosowania, przechowywania Aktualizacji dla własnych potrzeb Zamawiającego, zgodnie z jej charakterem i przeznaczeniem oraz warunkami Umowy,
      b) licencja udzielona zgodnie z lit. a może być wykorzystywana wyłącznie dla celów działalności Zamawiającego i nie obejmuje prawa do wprowadzania Aktualizacji do obrotu lub przekazywania ani w części ani w całości osobom trzecim zarówno odpłatnie, jak i nieodpłatnie w żadnej formie prawnej,
      c) w ramach udzielonej licencji Wykonawca upoważnia także Zamawiającego do korzystania z dokumentacji Aktualizacji dostępnej wraz z Aktualizacją, na polach eksploatacji wskazanych w lit. a,
      d) korzystanie z Aktualizacji wraz z ich dokumentacją następuje w ramach wynagrodzenia określonego w § 7 ust. 2 Umowy, bez konieczności ponoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat licencyjnych;
   2) przeniesienia Oprogramowania lub Aktualizacji na inną platformę systemową, jeżeli potrzeba taka po stronie Zamawiającego zaistnieje, oraz wsparcia technicznego udzielanego przez Wykonawcę w tym zakresie;
   3) asysty elektronicznej i telefonicznej w zakresie problemów dotyczących Oprogramowania lub Aktualizacji, zgłaszanych do Wykonawcy w Dni Robocze w godzinach 7:00 do 19.00 do działu Asysty Technicznej pod numer telefonu: ……, e-mail: ……;
   4) dostępu elektronicznego przez 24 godziny na dobę, 7 dni w tygodniu (poprzez serwis internetowy wskazany w ust. 2) do informacji na temat posiadanych przez Wykonawcę produktów Producenta, biuletynów technicznych, list dyskusyjnych, bazy danych problemów technicznych dotyczących Oprogramowania rejestrowanych przez pracowników działu Asysty Technicznej.
2. Wykonawca zobowiązuje się do zapewnienia Zamawiającemu dostępu do Aktualizacji poprzez serwis internetowy Producenta. Wykonawca zobowiązuje się do niezwłocznego, nie później niż 2 Dni Robocze od ich udostępnienia przez Producenta, informowania Zamawiającego o wszelkich Aktualizacjach udostępnionych przez Producenta, poprzez internetowy serwis Asysty Technicznej. Dostęp do Aktualizacji (wraz z jej dokumentacją) winien być zapewniony Zamawiającemu w terminie, w jakim Wykonawca zobowiązany jest do powiadomienia o udostępnieniu przez Producenta danej Aktualizacji.
3. W ramach Usługi Asysty Technicznej, Zamawiający ma dostęp do dokumentacji deweloperskiej (poradniki, instrukcje, opis API itp.) pomocnej w tworzeniu m.in. własnych zautomatyzowanych procesów biznesowych, rejestrów, raportów, portali użytkownika, wykresów i map.

## § 7

## Wynagrodzenie

1. Łączne wynagrodzenie z tytułu wykonania Umowy wynosi netto …….. zł (słownie: …….. złotych xx/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie: …….. złotych xx/100) zgodnie z formularzem ofertowym, stanowiącym załącznik nr 9 do Umowy.
2. Wynagrodzenie z tytułu świadczenia Usługi Asysty Technicznej w okresie wskazanym w § 2 ust. 1 pkt 1 Umowy wynosi netto …….. zł (słownie: …….. złotych xx/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie: …….. złotych xx/100).
3. Łączne wynagrodzenie z tytułu świadczenia Usługi Wsparcia w okresie wskazanym w § 2 ust. 1 pkt 1 Umowy wyniesie nie więcej niż netto …….. zł (słownie: …….. złotych xx/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie: …….. złotych xx/100), na które składa się:
   1) wynagrodzenie ryczałtowe z tytułu świadczenia Usługi Wsparcia, obejmującej zakres wskazany w załączniku nr 2 do Umowy oraz Warsztaty, o których mowa w § 5, wynoszące nie więcej niż netto …….. zł (słownie: …….. złotych xx/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie: …….. złotych xx/100), płatne w miesięcznych okresach rozliczeniowych;
   2) wynagrodzenie łączne z tytułu świadczenia konsultacji, w tym prac programistycznych w ramach Usługi Wsparcia wynoszące nie więcej niż netto …….. zł (słownie: …….. złotych xx/100) powiększone o należny podatek od towarów i usług (VAT), co daje kwotę wynagrodzenia brutto …… zł (słownie: …….. złotych xx/100), płatne zgodnie z ust. 7.
4. Wynagrodzenie jednostkowe z tytułu jednej godziny konsultacji, w tym prac programistycznych świadczonych w ramach Usługi Wsparcia wynosi netto: …….. (słownie: …… xx/100), powiększone o należny podatek od towarów i usług (VAT), co daje kwotę brutto …….. (słownie: …… xx/100).
5. Wynagrodzenie, o którym mowa w ust. 2 zostanie uiszczone z góry za każdy rok, przy czym zawarcie Umowy jest podstawą do wystawienia faktury VAT za pierwsze 12 miesięcy świadczenia Usługi Asysty Technicznej, zaś druga faktura może zostać wystawiona najwcześniej po roku od wystawienia pierwszej faktury.
6. Wynagrodzenie, o którym mowa w ust. 3 pkt 1 płatne będzie miesięcznie, na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie do 28 dni licząc od daty podpisania przez Zamawiającego Miesięcznego Protokołu Świadczenia Usług.
7. Wynagrodzenie Wykonawcy z tytułu realizacji konsultacji, w tym prac programistycznych świadczonych w ramach Usługi Wsparcia w danym miesiącu zostanie ustalone jako iloczyn faktycznie udzielonych godzin konsultacji lub prac programistycznych wynikających z Miesięcznego Protokołu Świadczenia Usług oraz stawki jednostkowej brutto za godzinę świadczenia Usługi Wsparcia. Wynagrodzenie miesięczne ustalone według powyższych zasad każdorazowo pomniejsza łączną kwotę wynagrodzenia wskazaną w ust. 3 pkt 2 Umowy.
8. W wynagrodzeniu, o którym mowa w ust. 2-4 zawierają się wszelkie koszty związane z wykonaniem przez Wykonawcę Umowy, w tym z tytułu udzielenia Zamawiającemu licencji uprawniającej do korzystania z Aktualizacji wraz z ich dokumentacją pozyskanych w trakcie świadczenia Usługi Asysty Technicznej oraz przeniesienia na Zamawiającego autorskich praw majątkowych do utworów wykonanych w ramach Usługi Wsparcia jak również wynagrodzenie z tytułu przeprowadzenia Warsztatów. Wykonawca przyjmuje do wiadomości, że wynagrodzenie określone w ust. 3 pkt 2 ma charakter maksymalny, a Zamawiający zastrzega sobie prawo do skorzystania ze świadczeń w zakresie Usług Wsparcia w liczbie mniejszej niż wynikałaby z kwoty wskazanej w ust. 3 pkt 2, zaś Wykonawcy w takim przypadku nie będzie przysługiwać jakiekolwiek roszczenie wobec Zamawiającego z tego tytułu. Wykonawcy przysługuje wynagrodzenie odpowiadające wyłącznie faktycznej liczbie zrealizowanych na rzecz Zamawiającego konsultacji w ramach poszczególnych okresów rozliczeniowych Usługi Wsparcia, obliczone zgodnie z ust. 7.
9. Błędnie wystawiona faktura VAT lub brak dokumentu stanowiącego podstawę wystawienia faktury spowoduje naliczenie ponownego 28 dniowego terminu płatności, od daty dostarczenia prawidłowo wystawionej faktury lub właściwego dokumentu stanowiącego podstawę do zapłaty.
10. Wykonawca jest uprawniony do wystawiania faktur VAT i posiada numer NIP: ……
11. Zapłata wynagrodzenia będzie dokonywana przelewem na rachunek bankowy Wykonawcy wskazany na fakturze. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Zamawiającego. W przypadku niezgodności, w dniu realizacji płatności, numeru rachunku bankowego wskazanego przez Wykonawcę na fakturze z numerem rachunku bankowego zamieszczonym w wykazie podmiotów, o których mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2020 r., poz. 106), Strony ustalają, że realizacja płatności nastąpi w trybie art. 108a ww. ustawy.
12. Jeżeli w trakcie realizacji Umowy nastąpi:
    1) zmiana stawki podatku od towarów i usług,

2) zmiana wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,

3) zmiana zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,

4) zmiana zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych

a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Wykonawcy określone w ust. 13-20 poniżej.

13. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.

14. Wykonawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 12 uprawniony jest do wystąpienia do Zamawiającego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 12 mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Wykonawcy określonego w Umowie, a w szczególności:

1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Wykonawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Wykonawcę.

2) przyjęte przez Wykonawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń- takimi jak np. umowy o pracę, dokumenty potwierdzające zgłoszenie pracowników do ubezpieczeń.

15. W terminie 30 dni od otrzymania wniosku o którym mowa w ust. 14, Zamawiający może zwrócić się do Wykonawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).

16. Zamawiający w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Wykonawcy.

17. Zamawiający najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 12 może przekazać Wykonawcy pisemny wniosek o dokonanie zmiany Umowy. Wniosek powinien zawierać co najmniej propozycję zmiany Umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.

18. Przed przekazaniem wniosku, o którym mowa w ust. 17, Zamawiający może zwrócić się do Wykonawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 12, mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Zamawiający. Postanowienia ust. 15-16 stosuje się odpowiednio, z tym, że Wykonawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Zamawiającego.

19. W przypadku niewykonania lub nienależytego wykonania przez Wykonawcę zobowiązania określonego w ust. 18 w terminie określonym w ust. 18, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 200,00 zł za każdy rozpoczęty dzień opóźnienia. Jeżeli w terminie określonym w ust. 18 Wykonawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 18 lub przedłożone przez Wykonawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Zamawiającego oceny, o której mowa w ust. 18 - Zamawiający wyznaczy Wykonawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Zamawiający uprawniony będzie do wypowiedzenia Umowy z zachowaniem miesięcznego terminu wypowiedzenia.

20. Jeżeli w trakcie procedury opisanej w ust. 14-19 zostanie wykazane, że zmiany, o których mowa w ust. 12 uzasadniają zmianę wysokości wynagrodzenia, Strony uzgodnią treść aneksu do Umowy oraz podpiszą aneks, z zachowaniem zasady zmiany wysokości wynagrodzenia w kwocie odpowiadającej zmianie kosztów wykonania Umowy wywołanych przyczynami określonymi w ust. 12.

## § 8

## Poufność

1. Wszelkie wiadomości, w których posiadanie wszedł Wykonawca przy zawieraniu i wykonywaniu Umowy jest on zobowiązany zachować w poufności. Wykonawca zobowiązuje się nie ujawniać ich osobom trzecim, wyjąwszy przypadki prawem przewidziane.

2. Wykonawca zobowiązuje się do pisemnego zobowiązania osób realizujących Umowę do zachowania w poufności wiadomości, o których mowa w ust. 1.

3. Powierzenie przetwarzania danych osobowych niezbędnych do realizacji Umowy, następuje na podstawie odrębnej umowy, której wzór zawiera załącznik nr 8 do Umowy. Dane osobowe z zasobów Zamawiającego mogą być przekazane podwykonawcy Wykonawcy jedynie na podstawie umowy powierzenia przetwarzania danych osobowych, której wzór zawiera załącznik nr 8A do Umowy.
4. Przed przystąpieniem do realizacji Umowy Wykonawca dostarczy Zamawiającemu wykaz podwykonawców, z którymi będą zawarte umowy powierzenia przetwarzania danych osobowych.
5. W przypadku, gdy na skutek nieprawidłowości w przetwarzaniu danych osobowych przez podwykonawcę zostanie mu naliczona przez Zamawiającego kara umowna lub Zamawiający będzie dochodzić od podwykonawcy odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego na podstawie odrębnej umowy zawartej zgodnie z załącznikiem nr 8A do Umowy – Zamawiający zastrzega sobie prawo do potrącenia naliczonej podwykonawcy kary umownej lub odszkodowania z wynagrodzenia należnego Wykonawcy lub do skorzystania z ze złożonego przez Wykonawcę zabezpieczenia należytego wykonania Umowy na co Wykonawca niniejszym wyraża zgodę.

**§ 9**

**Kary umowne**

1. Wykonawca zobowiązany jest do zapłaty na rzecz Zamawiającego kary umownej w wysokości 10 000,00 zł za każdy stwierdzony przypadek naruszenia zakazu, o którym mowa w § 3 ust. 2 Umowy.
2. W przypadku przekroczenia przez Wykonawcę czasu reakcji lub realizacji Naprawy Usterki/Awarii określonych w załączniku nr 2 do Umowy, Zamawiający ma prawo naliczenia kar umownych w wysokości 0,03% kwoty wynagrodzenia brutto określonego w § 7 ust. 1 Umowy za każdą rozpoczętą godzinę opóźnienia. Kara umowna jest naliczana osobno za każde nierozwiązane zgłoszenie.
3. W przypadku przekroczenia przez Wykonawcę czasu reakcji lubi realizacji Naprawy Usterki/Awarii powyżej 48 h, niezależnie od kary umownej opisanej w ust. 2, Zamawiający może rozwiązać Umowę w trybie natychmiastowym
4. W przypadku, gdy Wykonawca nie dotrzyma terminu udzielenia konsultacji w tym wykonania prac programistycznych, wynikającego z § 4 ust. 4 Umowy – Zamawiający wyznaczy Wykonawcy dodatkowy, nieprzekraczalny termin na rozwiązanie problemu zgłoszonego w trakcie konsultacji. Po bezskutecznym upływie tego terminu Zamawiający ma prawo naliczać karę umowną w wysokości 300,00 zł za każdą rozpoczętą godzinę opóźnienia. Jeżeli opóźnienie przekroczy 48 godzin, Zamawiający po bezskutecznym upływie tego terminu ma prawo naliczać karę umowną wskazaną w zdaniu poprzedzającym w podwójnej wysokości, do dnia udzielenia konsultacji lub wykonania/zrealizowania prac programistycznych włącznie.
5. W przypadku przekroczenia przez Wykonawcę terminu udostępnienia Aktualizacji, o którym mowa w §6 ust. 2, Umowy Zamawiający ma prawo naliczenia kary umownej w wysokości 0,05% kwoty wynagrodzenia brutto określonego w §7 ust. 1 Umowy za każdy rozpoczęty dzień opóźnienia.
6. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5 000,00 zł za każdy stwierdzony przypadek naruszenia zobowiązań określonych w § 3 ust. 4 lub ust. 6 Umowy, z wyjątkiem naruszeń w zakresie przetwarzania danych osobowych, za które odpowiedzialność reguluje odrębna umowa zawarta pomiędzy Stronami, stanowiącą załączniki nr 8 i nr 8A do Umowy (umowa powierzenia przetwarzania danych osobowych).
7. Jeżeli na skutek niewykonania bądź nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną w Umowie karę umowną, Zamawiającemu oprócz tej kary przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli szkoda powstanie z przyczyn innych niż te, ze względu, na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo do dochodzenia odszkodowania na zasadach ogólnych określonych w Kodeksie cywilnym.
8. Kary umowne płatne są w terminie 14 dni od daty otrzymania wezwania, przy czym Zamawiający zastrzega sobie prawo do potrącenia kary z wynagrodzenia za wykonanie Umowy, do czego Wykonawca upoważnia Zamawiającego.

**§ 10**

**Prawa autorskie**

1. Jeżeli w wyniku realizacji Usługi Wsparcia powstanie utwór w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, majątkowe prawa autorskie do utworu zostaną przeniesione na Zamawiającego w zakresie i w sposób opisany poniżej.
2. Wykonawca oświadcza i gwarantuje, że korzystanie przez Zamawiającego z wszelkich utworów powstałych w wyniku realizacji Usługi Wsparcia nie będzie naruszało praw osób trzecich, w szczególności praw autorskich oraz praw własności przemysłowej.
3. Wykonawca oświadcza, że przysługują mu wyłącznie i nieograniczone autorskie prawa majątkowe do utworów powstałych w trakcie realizacji Usługi Wsparcia oraz, że osoby uprawnione z tytułu osobistych praw autorskich do utworów powstałych w wyniku realizacji czynności zleconych nie będą wykonywać takich praw w stosunku do Zamawiającego.

4. Na podstawie Umowy, z chwilą powstania jakiegokolwiek utworu w wyniku realizacji którejkolwiek z czynności w ramach Usługi Wsparcia Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do powstałego utworu, na polach eksploatacji wskazanych w ust. 5 i 6, w ramach wynagrodzenia miesięcznego, ustalonego zgodnie z § 7 ust. 7 Umowy.
5. Przeniesienie autorskich praw majątkowych do utworów powstałych w wyniku realizacji Usługi Wsparcia, innych niż programy komputerowe, obejmuje następujące pola eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utrwalono – wprowadzanie do obrotu, użyczanie oraz najem oryginału oraz egzemplarzy;
   3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
   4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;
   5) tłumaczenie, przystosowanie, zmiany układu lub jakiekolwiek inne zmiany w utworze;
   6) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt 1-5.
6. Przeniesienie autorskich praw majątkowych do utworów powstałych w wyniku realizacji Usługi Wsparcia, będących programami komputerowymi, obejmuje następujące pola eksploatacji:
   1) trwałe i czasowe zwielokrotnianie utworów w całości lub części, jakimikolwiek środkami i w jakiejkolwiek formie, w tym do wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania, m.in. do systemu informatycznego, pamięci komputerów, sieci komputerowych;
   2) tłumaczenie, przystosowanie, zmiany układu lub jakiekolwiek inne zmiany w programie komputerowym, w tym łączenie w jeden system z innymi programami, z zachowaniem praw osoby, która tych zmian dokonała;
   3) rozpowszechnianie, w tym użyczanie, najem, dzierżawa, upoważnienie innych osób do wykorzystywania w całości lub części programu komputerowego lub jego kopii;
   4) modyfikacje kodu źródłowego;
   5) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt 1-4.
7. Z chwilą przekazania utworu będącego programem komputerowym Wykonawca każdorazowo przekaże Zamawiającemu kody źródłowe wraz z dokumentacją projektową, skrypty konfiguracyjne lub inne skrypty (np. budujące aplikację, instalacyjne, zasilające inicjalnie).
8. Z chwilą przekazania Zamawiającemu poszczególnych utworów wykonanych w ramach realizacji poszczególnych Usług, Zamawiający nabywa własność nośników, na których utwory te utrwalono, w ramach wynagrodzenia miesięcznego, ustalonego zgodnie z § 7 ust. 7 Umowy.

**§ 11**

**Zabezpieczenie należytego wykonania Umowy** (dalej: „**ZNWU**")

1. Wykonawca złożył u Zamawiającego ZNWU w wysokości _____ zł (słownie złotych: _____ 00/100) w jednej z form, o których mowa w art. 148 ust. 1 ustawy Prawo zamówień publicznych.
2. ZNWU dotyczy pokrycia ewentualnych roszczeń wynikających z niewykonania lub nienależytego wykonania Umowy.
3. ZNWU zostanie zwolnione (zwrócone) w terminie 30 dni od daty podpisania przez Zamawiającego Miesięcznego Protokołu Świadczenia Usług, o którym mowa w § 4 ust. 7 Umowy za ostatni miesiąc świadczenia Usługi Wsparcia.
4. W przypadku zmiany formy ZNWU w trakcie wykonywania Umowy stosuje się postanowienia ust. 5-10.
5. ZNWU w formie pieniężnej Wykonawca wpłaca przelewem na rachunek bankowy wskazany przez Zamawiającego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę _____ zł (słownie złotych: _____ xx/100), na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
7. ZNWU wnoszone w formie poręczenia ma być wystawione przez bank, spółdzielczą kasę oszczędnościowo-kredytową lub podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu

Polskiej Agencji Rozwoju Przedsiębiorczości, który poręczy należyte wykonanie umowy do wysokości _____ zł (słownie złotych: _____ xx/100).

8. W przypadku, gdy ZNWU będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, Zamawiający zastrzega sobie prawo do akceptacji projektu tych dokumentów.
9. ZNWU wniesione w formie pieniężnej podlega zwrotowi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek Wykonawcy.

   ZNWU w formie innej niż pieniężna Wykonawca złoży u Zamawiającego w Kancelarii Głównej, Warszawa ul. Poleczki 33, z dopiskiem „Dla Departamentu Informatyk

**§ 12**

**Postanowienia końcowe**

1. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Wszelkie zawiadomienia i oświadczenia woli wymienione w Umowie, niezależnie od nazwy pod którą występują, dla swojej skuteczności Strony muszą przekazać na piśmie osobiście za potwierdzeniem odbioru lub pocztą poleconą za zwrotnym poświadczeniem ich odbioru, chyba że Umowa przewiduje inaczej i będą uważane za skutecznie doręczone w dniu ich odbioru. Ustala się następujące dane adresowe:

   1) Zamawiający – Agencja Restrukturyzacji i Modernizacji Rolnictwa, Departament Informatyki

      ul. Poleczki 33, 02-822 Warszawa

   2) Wykonawca – ……
3. Zawiadomienia, zapytania, informacje niewymienione w postanowieniach Umowy mogą być przesyłane faksem, doręczane osobiście, przesyłane kurierem, listem lub za pośrednictwem poczty elektronicznej, pod warunkiem niezwłocznego potwierdzenia ich otrzymania przez odbiorcę. Zawiadomienia będą wysyłane na adresy lub numery faksów podane przez Strony. Każda ze Stron zobowiązana jest do niezwłocznego informowania drugiej Strony o każdej zmianie miejsca siedziby, adresu, adresu poczty elektronicznej lub numeru faksu. Zmiana adresów nie wymaga zachowania formy pisemnego aneksu do Umowy. Jeżeli Strona nie powiadomiła o zmianie miejsca siedziby, adresu, adresu poczty elektronicznej lub numeru faksu, zawiadomienia wysłane na ostatni znany adres, adres poczty elektronicznej lub numer faksu, Strony uznają za doręczone.
4. Wszelkie spory powstałe w związku z realizacją Umowy Strony poddadzą pod rozstrzygnięcie sądu powszechnego, miejscowo właściwego ze względu na siedzibę Zamawiającego.
5. Wykonawca nie może bez zgody Zamawiającego przenieść praw wynikających z Umowy na osoby trzecie (przelew).
6. Osobami upoważnionymi przez Strony do podpisywania protokołów określonych w Umowie oraz do rozpatrywania bieżących spraw związanych z wykonaniem Umowy, przy zachowaniu określonych w niej warunków, w tym terminów, są:

   po stronie Zamawiającego: ……

   po stronie Wykonawcy: …….

   Zmiana ww. osób nie stanowi zmiany Umowy wymagającej formy pisemnego aneksu.
7. W sprawach nieuregulowanych Umową zastosowanie mają w szczególności przepisy Kodeksu cywilnego.
8. Umowę sporządzono w czterech jednobrzmiących egzemplarzach, w tym trzy egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

**WYKONAWCA** **ZAMAWIAJĄCY**

***ZAŁĄCZNIK NR 1 DO UMOWY NR /DI/2020/2610 Z DNIA.....2020 R.***

**Wykaz Oprogramowania**

| **Product** | **APN Number** | **Maintenance Grants** |
|---|---|---|
| Genesys CIM Platform | 3GP21278ACAA | 35 |
| Genesys CPD/ASM | 3GP21282ACAA | 30 |
| Genesys Callback | 3GP21929ACAA | 30 |
| Genesys Chat | 3GP80855ACAA | 30 |
| Genesys Co-browse | 3GP21944ACAA | 30 |
| Genesys Customer Experience Insights | 3GP84586ACAA | 35 |
| Genesys E-mail | 3GP21059ACAA | 35 |
| Genesys Info Mart | 3GP21747ACAA | 35 |
| Genesys Outbound Voice | 3GP08809ACAA | 30 |
| Genesys SIP Interaction | 3GP09017ACAA | 35 |
| Genesys SMS | 3GP21886ACAA | 30 |
| Genesys Social Engagement Pkg | 3GP21219ACAA | 5 |
| Genesys Softphone | 3GP21208ACAA | 35 |
| Genesys Workforce Management | 3GP20738ACAA | 35 |
| Interaction Recording - Voice Edition | 3GP20166ACAA | 15 |
| Proactive Contact - E-mail/SMS | 3GP08822ACAA | 1 |
| SIP Qualification & Parking | 3GP21844ACAA | 18 |
| Workspace | 3GP20364ACAA | 35 |
| intelligent Workload Distribution & JMS Adapter | 3GP21286ACAA | 5 |
| RecViewer Voice recording | Custom | 35 |

***ZAŁĄCZNIK NR 1 A DO UMOWY NR /DI/2020/2610 Z DNIA.....2020 R.***

**Opis Systemu Contact Center**

**Ogólny opis systemu, którym dysponuje Zamawiający:**

1. System Contact Center obsługuje następujące kanały komunikacji:
    a. Głos przychodzący,
    b. Głos wychodzący,
    c. Poczta elektroniczna,
    d. Chat,
    e. SMS,
    f. Obsługa wniosków o oddzwonienie,
    g. Współdzielenie z klientem strony internetowej, na której przebywa klient,
    h. Kanały społecznościowe,
    i. Wielokanałowa aplikacja konsultanta spójna z aplikacją pracownika w oddziale,
    j. Widok interakcji obsługiwanych w oddziale.
2. System umożliwia dystrybucję zadań do pracowników terenowych. Dostępne kanały:
    a. Obsługa elektronicznej wersji wniosku,
    b. Widok interakcji obsługiwanych w Contact Center,
    c. Aplikacja pracownika w oddziale spójna z aplikacją konsultanta Contact Center.
3. System umożliwia identyfikację klienta poprzez obsługiwane kanały komunikacji.
4. System jest zainstalowany on-premise.
5. Skonfigurowano system raportów rzeczywistych oraz historycznych.
6. System umożliwia pojedyncze logowanie przez integrację z Active Directory (Kerberos 5, szyfrowanie AES-128) i wspiera mechanizmy SSO (single sign-on).
7. Uprawnienia użytkowników systemu bazują na modelu ról z możliwością konfiguracji dostępności funkcjonalności oraz ograniczania dostępu do zasobów/interakcji (w zależności od posiadanych uprawnień).
8. System umożliwia tworzenie logiki obsługi interakcji oraz wybór najlepszego konsultanta w jednym graficznym narzędziu dla wszystkich kanałów interakcji z klientem, w tym telefonu, e-maili, czatu, sms, facebooka, twittera, mesengera oraz składanych wniosków.
9. System umożliwia przedstawienie wszystkich kanałów interakcji z klientem, w tym telefonicznych, emailowych, czatowych, sms, facebooka, twittera, mesengera oraz składanych wniosków w jednym spójnym narzędziu raportowym.
10. Wybór najlepszego konsultanta – dla wszystkich kanałów – może odbywać się w oparciu o:
    a. Umiejętności,
    b. Profil,
    c. Dostępność,
    d. Lokalizację,
    e. Historię współpracy z klientem,
    f. Grafik dostępny w narzędziu systemu Contact Center.

    W przypadku nieznalezienia odpowiedniego konsultanta w oparciu o założone kryteria, system umożliwia przeprowadzenie kolejnego wyszukiwania według złagodzonych kryteriów.
11. System kierowania interakcji do konsultanta uwzględnia umiejętność konsultanta do jednoczesnej pracy z wieloma interakcjami, np. jedną rozmową telefoniczną, dwoma zadaniami i jednym chatem.
12. Aplikacja konsultanta umożliwia przełączanie się pomiędzy kanałami podczas obsługi interakcji, np. konsultant obsługujący wiadomość czat ma możliwość wykonania połączenia głosowego oraz napisania maila podczas czatowania z klientem.
13. Konsultanci w oddziałach i Contact Center mają dostęp do pełnej historii interakcji pomiędzy Zamawiającym a obsługiwanym Klientem, w tym wymienianych maili, czatów, sms i wiadomości Messenger.
14. Podczas pisania wiadomości chat lub email, strona www Zamawiającego ma możliwość podpowiadania odpowiedzi korzystając z Bazy Wiedzy.
15. Baza wiedzy jest udostępniona zarówno Klientowi na stronie www, jak i konsultantowi Contact Center.

***ZAŁĄCZNIK NR 2 DO UMOWY NR /DI/2020/2610 Z DNIA…….2020 r.***

# WARUNKI ŚWIADCZENIA USŁUGI WSPARCIA

1. Wykonawca zobowiązuje się do świadczenia, przez okres wskazany w § 2 ust 1 pkt 1 Umowy, Usługi Wsparcia dla Systemu CC przez wykwalifikowanych, polskojęzycznych inżynierów, posiadających wiedzę niezbędną do realizacji usług określonych w niniejszym załączniku.
2. W ramach Usługi Wsparcia Wykonawca zobowiązuje się do usuwania zgłoszonych Awarii/Usterek Systemu CC.
3. Wszelkie koszty Napraw realizowanych w ramach Usługi Wsparcia ponosi Wykonawca.
4. Zgłoszenia problemów związanych z nieprawidłowym działaniem Oprogramowania/Systemu CC w ramach Usługi Wsparcia będą dokonywane telefonicznie pod numerem: ……. lub pod adresem poczty elektronicznej: ……Tryb przyjmowania zgłoszeń: w Dni Robocze w godzinach 7:00 - 19:00 oraz w soboty w godzinach 10:00-16:00, przy czym zgłoszenia otrzymane po godzinie 19:00 lub w soboty po godzinie 16:00 będą traktowane jako zgłoszenia otrzymane rano, następnego Dnia Roboczego lub w sobotę. Wykonawca zobowiązany jest potwierdzić przyjęcie zgłoszenia drogą elektroniczną na e mail Zamawiającego_____ niezwłocznie, jednak nie później niż w ciągu 1 godziny od momentu jego otrzymania (czas reakcji). Niepotwierdzenie zgłoszenia w powyższym terminie Zamawiający uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu poczty elektronicznej lub numerów telefonów wskazanych powyżej, Wykonawca zobowiązany jest niezwłocznie powiadomić na piśmie Zamawiającego.
5. Wykonawca zobowiązuje się do świadczenia Usługi Wsparcia, z zachowaniem następujących terminów:

   a) czas reakcji - 1 godzina,

   b) czas realizacji (Awaria) – ……. godzin/y (*zgodnie z deklaracją Wykonawcy złożoną w pkt 5 Formularza Ofertowego*),

   c) czas realizacji (Usterka) – …… godzin/y (*zgodnie z deklaracją Wykonawcy złożoną w pkt 6 Formularza Ofertowego*),
   przy czym:

   **Awaria** oznacza stan niesprawności Systemu CC uniemożliwiający jego standardowe funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie - w odniesieniu do każdej z jego funkcjonalności.

   **Usterka** oznacza stan niesprawności Systemu CC pozwalający jednak na jego standardowe funkcjonowanie, lecz mający wpływ na komfort korzystania z niego przez użytkowników.

   **Naprawa** oznacza całkowite i skuteczne usunięcie Awarii/Usterki. Naprawa musi zapewnić powrót do poprawnego, w pełni zgodnego z przeznaczeniem, funkcjonowania Systemu CC.

   d) czas realizacji liczony jest od momentu potwierdzenia zgłoszenia Awarii/Usterki (zgodnie z pkt 4) do momentu potwierdzenia jej Naprawy przez Wykonawcę. Przez potwierdzenie Naprawy przez Wykonawcę Strony rozumieją potwierdzenie usunięcia Awarii/Usterki przesłane przez Wykonawcę na adres poczty elektronicznej Zamawiającego wskazany w pkt. 4. Jeśli po weryfikacji Zamawiający uzna, że dana Awaria/Usterka nie została usunięta to przysługuje mu prawo do zgłoszenia tego faktu w nowym zgłoszeniu Awarii/Usterki, przy czym czas jej trwania liczy się jako kontynuacja pierwotnie zgłoszonej i nie usuniętej Awarii/Usterki. Fakt Naprawy będzie odnotowywany każdorazowo w protokole, którego wzór stanowi załącznik nr 3 A do Umowy „Protokół Naprawy”**.**
6. Wykonawca zobowiązuję się do informowania na bieżąco Zamawiającego, za pomocą poczty elektronicznej (na adres poczty elektronicznej Zamawiającego wskazany w pkt. 4, o kolejnych etapach realizacji zgłoszenia Awarii/Usterki, w szczególności o wyniku analizy zgłoszenia, proponowanym rozwiązywaniu, wynikach testów i wdrożenia rozwiązania.

**ZAŁĄCZNIK NR 3A DO UMOWY NR /DI/2020/2610 Z DNIA .....2020 R.**

**PROTOKÓŁ NAPRAWY** (WZÓR)

Sporządzony w dniu ____ w związku ze zgłoszeniem z dnia __ na podstawie Umowy.....zawartą w dniu ..... pomiędzy ARiMR (**Zamawiającym**) a ..... (**Wykonawcą**)

Imię i nazwisko zgłaszającego:_____

Przedmiot Naprawy____

Opis zgłoszenia oraz Naprawy_____

Data zgłoszenia dokonania Naprawy_____

Termin realizacji zgłoszenia:

Zgłoszenie zostało wykonane w terminie / nie zostało wykonane w terminie*.

Opóźnienie wyniosło: …….. (liczba dni), …… (liczba godzin) *

Uwagi: ____*

Należy naliczyć karę umowną na podstawie § .... ust. ..... Umowy nr ……. z dnia ……. w wysokości ……..*

** niepotrzebne skreślić*

**Ze strony Wykonawcy:** **Ze strony Zamawiającego:**

**ZAŁĄCZNIK NR 3 DO UMOWY NR /DI/2020/2610 Z DNIA 2020 r.**

## MIESIĘCZNY PROTOKÓŁ ŚWIADCZENIA USŁUG (WZÓR)

Zgodnie z Umową.....zawartą w dniu ..... pomiędzy ARiMR (**Zamawiającym**) a ..... (**Wykonawcą**) Zamawiający *potwierdza należyte wykonanie/zgłasza uwagi do wykonania*[1] świadczonych w ramach realizacji Umowy czynności z zakresu Usługi Wsparcia, w okresie od dnia…….do dnia……..

W trakcie wymienionego okresu świadczenia Usługi Wsparcia udzielono … godzin konsultacji.

Opis konsultacji wraz z terminami: _____

W trakcie wymienionego okresu świadczenia Usługi Wsparcia Wykonawca zrealizował na rzecz Zamawiającego następujące prace programistyczne:( w tym mające charakter utworu, które zostały przez Zamawiającego odebrane bez zastrzeżeń i do których Zamawiający pozyskał autorskie prawa majątkowe zgodnie z warunkami Umowy):

- .....
- .....
- .....
- .....
- .....,

Liczba godzin pozostała do wykorzystania w ramach Umowy: .....

Przedmiot Umowy w zakresie objętym odbiorem został wykonany w terminie / nie został wykonany w terminie*.

Opóźnienie wyniosło: ……*

Uwagi: ……*

* niepotrzebne skreślić

**Ze strony Wykonawcy:** **Ze strony Zamawiającego:**

***ZAŁĄCZNIK NR 4 DO UMOWY ……./DI/2019/2610 Z DNIA……. 2020 R.***

## **Protokół przeprowadzenia Warsztatów** (wzór)

Zgodnie z Umową _____/DI/2020/2610 zawartą w dniu ..... 2020 r. pomiędzy ARiMR (**Zamawiającym**) a ..... (**Wykonawcą**) Zamawiający potwierdza, że Wykonawca przeprowadził Warsztaty , zgodnie z warunkami Umowy.

| **Wykonawca**<br>*(osoby upoważnione)* | **Zamawiający**<br>*(osoby upoważnione)* |
|---|---|
| …… | …… |
| ..... | ..... |

***ZAŁĄCZNIK NR 5 DO UMOWY ……./DI/2020/2610 Z DNIA……. 2020 R.***

*Załącznik nr 5 do Polityki bezpieczeństwa informacji w ARiMR*

**REGULAMIN UŻYTKOWNIKA**

**Spis treści:**

**§ 1.**
**Definicje**

Użyte w regulaminie określenia oznaczają:

1. dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);
2. hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
3. konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są powiązane z identyfikatorem użytkownika;
4. spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;
5. uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby/podmiotu;
6. urządzenie przenośne – urządzenie mobilne takie jak laptop, notebook, netbook, palmtop, tablet, telefon komórkowy, smartfon, MDA/PDA, pendrive, odtwarzacz mp3/4, aparat cyfrowy, czytnik kart pamięci, urządzenie do nawigacji GPS itp.

**§ 2.**
**Szkolenia dla użytkowników systemów teleinformatycznych**

1. Szkolenia użytkowników systemów teleinformatycznych mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić systemy teleinformatyczne.
2. Warunkiem uzyskania podstawowego dostępu do systemu teleinformatycznego Agencji (konto domenowe i konto pocztowe) przez pracownika jest odbycie szkolenia wstępnego przeprowadzanego przez bezpośredniego przełożonego potwierdzone podpisem pracownika na wniosku o przyznanie dostępu, którego wzór zawarto w Książce Procedur KP-611-101-ARiMR – „Obsługa kont użytkowników systemów informatycznych ARiMR”.
3. Warunkiem uzyskania dostępu do zaawansowanych funkcjonalności systemów teleinformatycznych Agencji jest odbycie szkoleń i zdanie egzaminów zgodnych z wymaganiami stawianymi przez Właścicieli Zasobów teleinformatycznych.
4. Szkolenia i egzaminy sprawdzające powinny być okresowo powtarzane (częstotliwość takich szkoleń określają Właściciele Zasobów teleinformatycznych) ze szczególnym uwzględnieniem:
    1) zmian dokonywanych w systemach teleinformatycznych, mających wpływ na sposób korzystania z tych systemów przez użytkowników,
    2) zmian przepisów prawa oraz uregulowań wewnętrznych,
    3) wystąpienia przypadków naruszenia bezpieczeństwa, słabości systemu lub zidentyfikowanych błędów systemów teleinformatycznych.
5. Okresowo (nie rzadziej niż raz na rok) przeprowadza się szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia te obejmują zagadnienia ujęte w niniejszym Regulaminie, a w szczególności dotyczą:
    1) zapoznania z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji, w tym z obowiązującą w Agencji polityką bezpieczeństwa informacji oraz polityką systemu zarządzania bezpieczeństwem informacji,
    2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu, systemów operacyjnych, aplikacji, itp.),
    3) sposobu postępowania w przypadku zdarzenia związanego z naruszeniem bezpieczeństwa informacji,
    4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.
6. Szkolenia doskonalące w zakresie obowiązujących w Agencji regulaminów związanych z bezpieczeństwem informacji mogą być przeprowadzane w zależności od zakresu obowiązków danego użytkownika przez:
    1) Administratora Systemu,
    2) Inspektora Bezpieczeństwa Informacji,
    3) Administratora Zabezpieczeń Fizycznych,
    4) Właściciela Procesu / Właściciela Zasobu,
    5) Bezpośredniego przełożonego.
7. Szkolenia doskonalące powinny kończyć się testem sprawdzającym zrozumienie przekazanych informacji adekwatnym do poziomu i zakresu prowadzonego szkolenia.
8. Uczestnictwo w szkoleniu każdy użytkownik potwierdza podpisem na liście obecności, z wyjątkiem szkoleń, które odbywają się w formie e-learning.

9. Szkolenia i egzaminy związane z użytkowaniem systemów teleinformatycznych są odnotowywane w Systemie e-szkoleń ARiMR.
10. Nieprzystąpienie do szkolenia, o którym mowa w § 2 ust. 5 lub niezaliczenie testu, o którym mowa w § 2 ust. 7, w terminie podstawowym i dodatkowym skutkuje blokadą dostępu do systemu teleinformatycznego Agencji na wniosek dyrektora komórki właściwej ds. bezpieczeństwa informacji.
11. Przywrócenie dostępu do systemu teleinformatycznego następuje na wniosek przełożonego użytkownika, zgodnie z procedurą zawartą w KP-611-101-ARiMR, po wcześniejszym odbyciu dodatkowego szkolenia doskonalącego i pozytywnym zaliczeniu testu.

**§ 3.**
**Używanie autoryzowanych środków do przetwarzania informacji**

1. Środki do przetwarzania informacji wykorzystywane w Agencji są przeznaczone wyłącznie do wykonywania zadań służbowych.
2. Każdy środek do przetwarzania informacji podlega inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym Agencji) zgodnie z zasadami określonymi w odrębnych dokumentach Agencji.
3. Wykorzystywanie środków do przetwarzania informacji, będących własnością Agencji, w celach niezwiązanych z powierzonymi obowiązkami wymaga uzgodnienia z bezpośrednim przełożonym i, jeżeli zachodzi taka potrzeba wynikająca z zakresu ewentualnego wykorzystania urządzeń, z Administratorem Systemu.
4. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nie posiadających autoryzacji.
5. Użytkownicy mogą korzystać ze stacji roboczych wyłącznie na stanowiskach im przydzielonych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą i na polecenie bezpośredniego przełożonego lub w przypadkach opisanych w Planach Zapewnienia Ciągłości Działania Agencji.
6. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
7. W przypadku korzystania ze stacji roboczej przez kilku użytkowników, kierownik komórki bądź jednostki organizacyjnej wyznacza osobę odpowiedzialną za sprzęt, określając jednocześnie uprawnienia i obowiązki wszystkich współużytkowników tego sprzętu.
8. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia systemów teleinformatycznych.
9. Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji systemu teleinformatycznego.
10. Nośniki uszkodzone, wycofywane z eksploatacji lub przekazywane do ponownego użycia użytkownik przekazuje Administratorowi Systemu odpowiedzialnemu za przeprowadzenie zniszczenia lub trwałego skasowania danych, korzystając z następujących procedur:
    1) programowego kasowania danych na dyskach twardych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,
    2) niszczenia zawartości komputerowych nośników magnetycznych – zamieszczonej w Książce Procedur KP-611-204-ARiMR,
    3) niszczenia nośników optycznych – zamieszczonej w Książce Procedur KP-611-186-ARiMR.
11. Postanowienia ust. 10 nie ograniczają ani nie wykluczają stosowania obowiązujących w Agencji zasad dotyczących gospodarowania środkami trwałymi oraz wyposażeniem.

**§ 4.**
**Wynoszenie mienia i korzystanie z urządzeń przenośnych**

1. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem (hasło na BIOS). Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
2. Wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów przenośnych, reguluje procedura wydawania zezwoleń na wynoszenie sprzętu komputerowego z ARiMR zawarta w Książce Procedur KP-611-206-ARiMR.
3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów, salach konferencyjnych oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.

4. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją, jeśli pozostają w postaci niezaszyfrowanej.

5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza strefą administracyjną Agencji, obowiązany jest do wystąpienia do Administratora Systemu z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne określone w Polityce kryptografii oraz ochronę antywirusową.

6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza Agencją użytkownik niezwłocznie powiadamia o tym fakcie Help Desk ARiMR oraz bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłasza ten fakt na policję. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

**§ 5.**
**Korzystanie z systemów teleinformatycznych Agencji oraz Internetu**

1. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych realizowane jest w oparciu o następujące zasady:
   1) „minimalnych przywilejów" – każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,
   2) „wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
   3) „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.
4. Każdy użytkownik ma w systemie unikalny identyfikator.
5. Przed uzyskaniem dostępu do systemów teleinformatycznych Agencji użytkownik jest informowany przez bezpośredniego przełożonego o zakresie przyznawanych mu uprawnień.
6. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
7. Jeżeli w trakcie korzystania z zasobów systemu teleinformatycznego użytkownik stwierdzi, że posiadane uprawnienia wykraczają poza przyznane, zobowiązany jest niezwłocznie zgłosić ten fakt do Help Desk ARiMR. Nie dokonanie zgłoszenia tego faktu może zostać potraktowane jako celowe i świadome naruszenie praw dostępu.
8. Po stwierdzeniu posiadania większych uprawnień zabronione jest ich testowanie i wykorzystywanie.
9. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się. Ponadto, użytkownik każdorazowo w przypadku oddalenia się od stacji roboczej obowiązany jest zablokować system.
10. Na użytkowniku spoczywa obowiązek zabezpieczenia opracowywanych bądź tworzonych przez siebie danych przed utratą. Również wszelkie dane źródłowe, na których użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.
11. Użytkownik ma następujące możliwości zabezpieczenia danych (plików) przed utratą:
    1) umieszczenie danych na serwerze plików (fileserver) – jest to zalecana forma zabezpieczenia danych,
    2) sporządzenie kopii zapasowej na wymiennym nośniku komputerowym,
    3) sporządzenie wydruków z wyniku pracy nad przetwarzanymi danymi.
12. Niedopuszczalne jest umieszczanie na serwerze plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
13. W przypadku potrzeby zabezpieczenia plików o dużych rozmiarach należy skorzystać z procedury nagrywania danych na nośnikach optycznych zawartej w Książce Procedur KP-611-186-ARiMR - „Postępowanie z optycznymi nośnikami danych".
14. Zabronione jest:
    1) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
    2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika,
    3) korzystanie z konta innego użytkownika, chyba że część lub całość zasobów związanych z tym kontem są udostępniane zgodnie z zasadami obowiązującymi w Agencji,
    4) przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne,

5) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych wewnętrznych jak również zewnętrznych, nie należących do Agencji,
6) udzielanie informacji o zasadach ochrony systemów teleinformatycznych Agencji, w tym o identyfikatorach używanych w tych systemach,
7) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych,
8) świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemach teleinformatycznych,
9) świadome wprowadzanie błędnych danych do systemów teleinformatycznych,
10) udostępnianie danych osobom nieupoważnionym,
11) włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,
12) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne,
13) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego przez Komitet oprogramowania i danych,
14) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

**§ 6.**
**Korzystanie z poczty elektronicznej i innych elektronicznych systemów komunikacyjnych**

1. Wszyscy pracownicy Agencji mają dostęp do wewnętrznej poczty elektronicznej.

2. Agencyjna poczta służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych Agencji podlega rejestrowaniu i filtrowaniu, o którym mowa w ust. 3.

3. Użytkownicy są świadomi, że wiadomości elektroniczne niezwiązane z działalnością Agencji, a zawierające słowa bądź temat uznane za niedozwolone, zgodnie z zasadami filtrowania komunikacji niepożądanej obowiązującymi w Agencji, będą zatrzymywane i następnie usuwane z systemu pocztowego.

4. Zalecanym formatem przesyłanych wiadomości jest „zwykły tekst". O ile nie jest to konieczne, nie należy tworzyć wiadomości w formacie HTML.

5. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

6. Zabronione jest:

1) rozsyłanie z komputerów Agencji oraz przyznanych użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą, wyjątek stanowią komunikaty niestandardowe rozsyłane zgodnie z „Zasadami świadczenia przez Departament Informatyki usługi dystrybucji komunikatów do dużych grup odbiorców",
2) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),
3) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Agencji,
4) odbieranie przesyłek z nieznanych źródeł,
5) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,
6) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych,
7) ukrywanie lub dokonywanie zmian tożsamości nadawcy,
8) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
9) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu poczty elektronicznej na adres e-mail: spam@arimr.gov.pl,
10) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy,
11) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Agencji lub do poszukiwania dodatkowego zatrudnienia.

**§ 7.**
**Ochrona haseł i kluczy kryptograficznych**

1. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.

2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

3. Każdy użytkownik posiadający dostęp do systemów teleinformatycznych Agencji zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie teleinformatycznym Agencji,
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia,
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu,
   4) poinformowania Administratora Systemu oraz Inspektora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła,
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych,
   6) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
4. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach,
   4) udostępnianie haseł innym użytkownikom,
   5) przeprowadzanie prób łamania haseł,
   6) wpisywanie haseł „na stałe" (np. w skryptach logowania).
5. W zależności od funkcjonujących w Agencji systemów operacyjnych i aplikacji zasady określone w ust. 3 pkt 3, 5 i 6 oraz ust. 4 pkt 2 i 3 mogą być wymuszane ustawieniami systemu teleinformatycznego wprowadzanymi przez Administratora Systemu na podstawie zasad określonych w odrębnych dokumentach Agencji.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania z uwzględnieniem wymagań określonych w Polityce kryptografii, w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu oraz Inspektorowi Bezpieczeństwa Informacji.

**§ 8.**

**Zgodność oprogramowania z prawami autorskimi**

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania.
2. Użytkownikowi nie wolno:
   1) uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone na danej stacji roboczej,
   2) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw do własności intelektualnej,
   3) kopiować i rozprowadzać bez upoważnienia oprogramowania stworzonego w Agencji lub na potrzeby Agencji,
   4) samodzielnie usuwać oprogramowania, którego używa.
3. Każdy plik znajdujący się:
   1) na wymiennym nośniku komputerowym,
   2) otrzymany za pomocą poczty elektronicznej lub pobrany z Internetu,

   podlega sprawdzeniu za pomocą oprogramowania antywirusowego zainstalowanego na komputerze przypisanym do użytkownika.
4. W przypadku wykrycia jakichkolwiek plików lub oprogramowania innego niż to, które znajduje się w spisie, Administrator Systemu ma prawo do natychmiastowego ich skasowania bez uzgodnienia z użytkownikiem.
5. O przypadkach używania nieautoryzowanego oprogramowania Administrator Systemu informuje Inspektora Bezpieczeństwa Informacji.
6. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nielegalnego oprogramowania w przypisanym mu komputerze, jeśli nie dopełnił obowiązków wskazanych w niniejszym Regulaminie.

**§ 9.**
**Korzystanie z urządzeń komunikacji głosowej, faksowej i wizyjnej**

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji wrażliwych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje wrażliwe jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

**§ 10.**
**Zasady „czystego biurka i czystego ekranu"**

1. Palenie, jedzenie oraz picie na stanowiskach komputerowych oraz w pomieszczeniach, w których znajdują się środki przetwarzania informacji (pomieszczenia serwerowni i węzłów teletechnicznych) jest zabronione.
2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:
   1) przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych,
   2) nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,
   3) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer, niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,
   4) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów zawierających informacje wrażliwe,
   5) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu,
   6) używać wygaszaczy ekranu zabezpieczonych hasłem,
   7) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu hasła,
   8) ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,
   9) odpowiednio zabezpieczyć miejsca przyjmowania/wysyłania korespondencji papierowej oraz odbioru/wysyłania faksów,
   10) włączać blokadę urządzeń kopiujących, zabezpieczając je w ten sposób przed nieuprawnionym użyciem,
   11) zwracać uwagę i powodować usuwanie pozostawionych oryginałów lub kopii w pobliżu urządzeń kserograficznych,
   12) zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru,
   13) nie pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach,
   14) niszczyć niepotrzebne nośniki papierowe w niszczarkach, jak np. dokumenty błędnie wydrukowane, powielone kopie itp. (za wyjątkiem nośników zawierających informacje wrażliwe, których sposób niszczenia regulują odrębne przepisy, w tym przepisy kancelaryjno-archiwalne Agencji w zakresie brakowania dokumentacji niearchiwalnej).
3. W uzasadnionych przypadkach realizacji zadań wymagających nieprzerwanego dostępu do zasobów teleinformatycznych (np. długotrwałe wgrywanie patch'y, pobieranie dużych ilości danych, odbywające się poza godzinami pracy ze względu na przepustowość łącz, wydajność baz danych, itp.) dopuszczalne jest, w porozumieniu z komórką właściwą ds. informatyki, odstąpienie od wymogu podanego w ust. 2 pkt 3.

**§ 11.**
**Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego**

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji.

2. Do przypadków mogących świadczyć lub świadczących o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się:

    1) nieautoryzowany dostęp do danych,
    2) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna, itp.),
    3) utratę usługi, urządzenia lub funkcjonalności,
    4) nieautoryzowaną modyfikację lub zniszczenie danych,
    5) udostępnienie informacji wrażliwych osobom nieupoważnionym,
    6) pozyskiwanie oprogramowania z nielegalnych źródeł,
    7) pojawianie się nietypowych komunikatów na ekranie,
    8) niemożność zalogowania się do systemu teleinformatycznego,
    9) spowolnienie pracy oprogramowania,
    10) niestabilna praca systemu teleinformatycznego,
    11) brak reakcji systemu na działania użytkownika,
    12) ponowny start lub zawieszanie się komputera,
    13) ograniczenie funkcjonalności oprogramowania.

3. Za naruszenie zasad ochrony informacji wrażliwych uważa się w szczególności:

    1) nieupoważniony dostęp, modyfikację, kopiowanie, udostępnienie lub zniszczenie /usunięcie informacji wrażliwych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych,
    2) udostępnianie informacji wrażliwych nieuprawnionym podmiotom,
    3) nieautoryzowany dostęp do danych przez połączenie sieciowe,
    4) niedopełnienie obowiązku ochrony informacji wrażliwych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, nie zablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się informacje wrażliwe),
    5) stworzenie niezabezpieczonego kanału dystrybucji informacji wrażliwych,
    6) nielegalne bądź nieświadome ujawnienie informacji wrażliwych,
    7) pozyskiwanie informacji wrażliwych z nielegalnych źródeł,
    8) przetwarzanie informacji wrażliwych niezgodne z uprawnionym celem i zakresem,
    9) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego,
    10) ujawnienie indywidualnych haseł dostępu do informacji wrażliwych w systemie,
    11) przesyłanie informacji wrażliwych przez Internet bez zabezpieczenia,
    12) przesyłanie dokumentów papierowych i nośników elektronicznych z informacja-mi wrażliwymi bez zabezpieczenia,
    13) wykonanie nieuprawnionych kopii informacji wrażliwych,
    14) kradzież nośników zawierających informacje wrażliwe lub oprogramowanie,
    15) kradzież sprzętu służącego do przetwarzania informacji wrażliwych,
    16) spowodowanie utraty informacji wrażliwych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
    17) dopuszczenie do braku aktualnych kopii bezpieczeństwa informacji wrażliwych lub brak odpowiednich nośników do sporządzania kopii,
    18) niewłaściwe niszczenie nośników z informacjami wrażliwymi pozwalające na ich odczyt,
    19) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się informacje wrażliwe,
    20) dopuszczenie do przetwarzania informacji wrażliwych pracowników bez odpowiednich upoważnień,
    21) nie przeszkolenie pracowników w zakresie zasad bezpieczeństwa informacji wrażliwych,
    22) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa informacji wrażliwych w Agencji.

4. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.

5. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Administratora Systemu lub Inspektora Bezpieczeństwa Informacji lub Administratora Zabezpieczeń Fizycznych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.

6. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędów lub awarii systemu użytkownik:

1) zabezpiecza dostęp do miejsca lub urządzenia w sposób umożliwiający odtworzenie okoliczności naruszenia bezpieczeństwa lub niewłaściwego funkcjonowania oprogramowania,
2) wstrzymuje pracę na stacji roboczej i odseparowuje komputer od sieci,
3) niezwłocznie informuje Help Desk ARiMR (w przypadku wystąpienia zdarzenia związanego z systemem teleinformatycznym) lub Administratora Zabezpieczeń Fizycznych (jeżeli zdarzenie dotyczy bezpieczeństwa fizycznego i środowiskowego), a także bezpośredniego przełożonego,
4) niezależnie od zapisów pkt 3) niezwłocznie informuje Inspektora Ochrony Danych oraz Inspektora Bezpieczeństwa Informacji w przypadku naruszenia zasad ochrony danych osobowych przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,
5) w przypadku zakwalifikowania przez IBI danego zdarzenia jako incydent, wypełnia w porozumieniu z nim część A raportu o incydencie bezpieczeństwa informacji (wzór raportu określa załącznik nr 3 do Regulaminu zarządzania incydentami).

**§ 12.**
**Postępowanie dyscyplinarne w przypadku naruszenia bezpieczeństwa**

1. Nieprzestrzeganie zasad określonych w dokumentach określających politykę bezpieczeństwa informacji stosowanych na danym stanowisku pracy przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej określonej w Regulaminie pracy.
2. Każdy przypadek wskazany w ust. 1 jest analizowany przez Inspektora Bezpieczeństwa Informacji, który w porozumieniu z Administratorem Systemu, Administratorem Zabezpieczeń Fizycznych oraz bezpośrednim przełożonym użytkownika, dokonuje kwalifikacji naruszenia. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Każdy przypadek naruszenia bezpieczeństwa informacji zgłaszany jest niezwłocznie dyrektorowi komórki właściwej ds. bezpieczeństwa informacji i opisywany zgodnie z Regulaminem zarządzania incydentami.

*Załącznik nr 8 do Polityki bezpieczeństwa informacji w ARiMR*

# REGULAMIN ZARZĄDZANIA INCYDENTAMI

**Spis treści:**

**§ 1.**
**Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji**

1. Wszyscy pracownicy Agencji oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów teleinformatycznych Agencji i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury Agencji dotyczące bezpieczeństwa informacji.

2. Zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji opisane zostały w Regulaminie użytkownika.

3. Osoba dokonująca zgłoszenia jest informowana przez Inspektora Bezpieczeństwa Informacji/Administratora Zabezpieczeń Fizycznych/Help Desk ARiMR o wyniku obsługi zgłoszenia.

4. Administrator Systemu/Administrator Zabezpieczeń Fizycznych ma obowiązek zareagować na alarm wygenerowany przez moduł automatycznego powiadamiania w systemach wykrywania włamań (systemów teleinformatycznych oraz elektronicznych systemów zabezpieczeń). W razie zidentyfikowania zagrożenia naruszenia bezpieczeństwa ochrony danych osobowych Administrator Systemu/Administrator Zabezpieczeń Fizycznych niezwłocznie informuje Inspektora Ochrony Danych, przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,

5. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi podmiotom zewnętrznym, powiadamianie Administratora Systemu/Administratora Zabezpieczeń Fizycznych/ Inspektora Bezpieczeństwa Informacji/ Inspektora Ochrony Danych o zdarzeniu odbywa się na zasadach określonych w umowie o świadczeniu usług.

6. W celu zapewnienia prawidłowości i kompletności zgłaszania oraz obsługi zdarzeń związanych z bezpieczeństwem informacji, dyrektor komórki właściwej ds. bezpieczeństwa informacji dokonuje:

   1) comiesięcznych analiz z użyciem raportów tworzonych w ramach realizacji umów z podmiotami zewnętrznymi;

   2) przeglądu zdarzeń z wykorzystaniem, udostępnionych przez komórkę właściwą ds. informatyki, narzędzi monitorujących środowisko teleinformatyczne Agencji w czasie rzeczywistym.

**§ 2.**
**Postępowanie z incydentami**

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych lub pracownik Help Desk ARiMR dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:

   1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna;

   2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;

   3) awaria techniczna czasowo blokująca dostępność informacji;

   4) incydent niskiej kategorii - związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności i poufności, nie generujący kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego Agencji;

   5) incydent średniej kategorii – związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi nie przekraczającymi kwoty 137 tys. € oraz możliwością konsekwencji prawnych i/lub utraty wizerunku;

   6) incydent wysokiej kategorii - związany z naruszeniem bezpieczeństwa informacji, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów Agencji; skutki tego incydentu powodują uruchomienie PZCD i wznowienie funkcjonowania w Zapasowych Miejscach Pracy; incydentem wysokiej kategorii jest również incydent, którego skutki mogą spowodować straty przekraczające kwotę 137 tys. €.

2. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do przekazania informacji oraz opinii w wyznaczonym przez Inspektora Ochrony Danych terminie.

3. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa informacji mogą świadczyć:

1) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;

2) niestabilna praca systemu teleinformatycznego;

3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);

4) nowe „podejrzane" (nieznane) konta użytkowników;

5) wysoka aktywność kont, które długo pozostawały niewykorzystane;

6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;

7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);

8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Agencji (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

4. O zdarzeniu noszącym znamiona incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych/pracownik Help Desk ARiMR powiadamia niezwłocznie Inspektora Bezpieczeństwa Informacji (IBI), który dokonuje ostatecznej jego klasyfikacji.

5. Inspektor Bezpieczeństwa Informacji, we współpracy z Administratorem Systemu oraz, jeśli zachodzi taka potrzeba, z Administratorem Zabezpieczeń Fizycznych, przeprowadza analizę incydentu.

6. Analiza incydentu uwzględnia następujące kryteria:

1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego;

2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.);

3) liczba jednostek/komórek organizacyjnych Agencji, zakres zasobów dotkniętych incydentem;

4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji;

5) możliwości rozszerzania się incydentu i sposoby jego ograniczania;

6) szacowany poziom szkód finansowych;

7) rodzaj ujawnionej informacji (jeśli ma zastosowanie – np. dane osobowe);

8) szacunkowy czas, po którym skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji;

9) skutki organizacyjne i prawne (wstępny szacunek).

7. W przypadku, gdy incydent ma skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej Agencji, dyrektor komórki właściwej ds. bezpieczeństwa informacji informuje niezwłocznie Prezesa Agencji.

8. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako incydentu wysokiej kategorii, dyrektor komórki właściwej ds. bezpieczeństwa informacji powiadamia niezwłocznie Prezesa Agencji.

9. W przypadku, gdy zasięg incydentu wykracza poza system teleinformatyczny Agencji, Administrator Systemu, w porozumieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi podmiotami zewnętrznymi, może przekazać do podmiotu zewnętrznego informacje o incydencie zawierające:

1) typ zdarzenia;

2) informacje o odległym systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników;

3) wszystkie zapisy z rejestrów zdarzeń w określonym przedziale czasowym;

4) inne informacje określone w umowie z podmiotem zewnętrznym.

10. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Prezes Agencji.

**§ 3.**
**Postępowania Inspektora Ochrony Danych w toku obsługi incydentów**

1. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do niezwłocznego przekazania informacji oraz opinii.

2. W wyniku analizy Inspektor Ochrony Danych stwierdza czy jest prawdopodobne, że stwierdzony incydent skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych oraz szacuje ryzyko z tym związane.

3. W przypadku stwierdzenia wysokiego ryzyka naruszenia praw i wolności osób fizycznych Inspektor Ochrony Danych informuje o tym Prezesa ARiMR.

4. Inspektor Ochrony Danych odpowiada za dokonanie czynności zgłoszenia stwierdzonego incydentu naruszenia ochrony danych osobowych, w którym wystąpiło wysokie ryzyko naruszania praw i wolności osób fizycznych, do Urzędu Ochrony Danych Osobowych.

5. Inspektor Ochrony Danych pełni nadzór nad właściwym dokonaniem procesu poinformowania właścicieli danych osobowych, których dotyczy incydent, przez odpowiednie jednostki, komórki organizacyjne Agencji. Informacje z pełnionego nadzoru przekazuje Prezesowi ARiMR oraz Komitetowi Sterowania Bezpieczeństwem Informacji.

6. Inspektor Ochrony Danych prowadzi Rejestr incydentów naruszeń ochrony danych osobowych, o których mowa w ust. 3.

**§ 4.**
**Ograniczanie skutków incydentu**

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych prowadzi bieżącą dokumentację incydentu. Dokumentacja ta w szczególności obejmuje:
   1) wszystkie zdarzenia zachodzące w systemie informacyjnym (zapisy systemowych dzienników audytu zdarzeń i dzienników audytu, lub zapisy z elektronicznych systemów zabezpieczeń);
   2) wszystkie podejmowane działania (opatrzone datą i czasem);
   3) wszystkie przeprowadzone rozmowy (osoba rozmówcy, data i czas zdarzenia, treść rozmowy).

2. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowanie przy postępowaniu z incydentem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego), bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

3. Administrator Systemu/Administrator Zabezpieczeń Fizycznych przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowania źródła naruszenia bezpieczeństwa. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.

4. W przypadku, gdy działania opisane w ust. 3 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Agencji, Administrator Systemu/Administrator Zabezpieczeń Fizycznych przedstawia decyzję do akceptacji Prezesa Agencji, wraz z rekomendacją dyrektora komórki właściwej ds. bezpieczeństwa informacji.

5. Rekomendacja dyrektora komórki właściwej ds. bezpieczeństwa informacji uwzględnia:
   1) uzależnienie Agencji od systemu teleinformatycznego (jak długo Agencja może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu);
   2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych Agencji na ujawnienie w przypadku utrzymywania się stanu naruszenia zabezpieczenia;
   3) stopień uświadomienia użytkowników (jaka może być reakcja użytkowników na anormalne zachowanie się systemu – np. niemożność zarejestrowania się, wyłączenie niektórych funkcji, itp.);
   4) konieczność schwytania i ewentualnego ukarania sprawcy (przy założeniu, że istnieją okoliczności umożliwiające takie działanie);
   5) konieczność angażowania zasobów systemu informatycznego (jaka część i jak długo);
   6) aspekt finansowy, organizacyjny i ludzki podejmowanych działań (jak długo działanie ma trwać, w jakim stopniu zakłóca normalne funkcjonowanie Agencji, jakie są tego koszty).

6. Przy ograniczaniu skutków incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji, może korzystać z konsultantów zewnętrznych, jeśli Agencja wcześniej zawarła w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji Agencji.

**§ 5.**
**Odtwarzanie systemu informacyjnego**

1. Z zastrzeżeniem ust. 4, Administrator Systemu przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.
2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Zapewnienia Ciągłości Działania ARiMR, odtwarzanie systemu jest realizowane w oparciu o procedury opisane w tym planie.
3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemu ma uzasadnioną pewność, że nie zawiera źródła incydentu.
4. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
5. Prezes Agencji, po zasięgnięciu opinii dyrektora komórki właściwej ds. bezpieczeństwa informacji i Administratora Systemu, może podjąć decyzję o podjęciu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

**§ 6.**
**Działania po zakończeniu incydentu**

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, przy wsparciu Administratora Systemu, Właścicieli Procesów / Właścicieli Zasobów, Administratora Zabezpieczeń Fizycznych, sporządza raport z incydentu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego regulaminu, oraz przedstawia go Komitetowi.
2. Jeśli zachodzi taka potrzeba, to Administrator Systemu/ Administrator Zabezpieczeń Fizycznych sporządza dodatkowy raport techniczny, stanowiący załącznik do raportu wskazanego w ust. 1 i zawierający co najmniej:
   1) rejestr incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań;
   2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód);
   3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu;
   4) kopię dziennika pracy systemu z okresu trwania incydentu;
   5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu;
   6) zakres informacji technicznych przekazanych Podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji przedkłada Prezesowi Agencji rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości.

**§ 7.**
**Rejestrowanie informacji o incydentach**

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi rejestr incydentów zawierający następujące informacje:
   1) opis incydentu;
   2) datę i godzinę zgłoszenia incydentu;
   3) dane identyfikujące osobę zgłaszającą;
   4) dane osoby przekazującej informację o incydencie;
   5) datę zarejestrowania incydentu;
   6) dane identyfikujące osobę rejestrującą incydent;
   7) informację o zgromadzonych materiałach dowodowych;
   8) informacje dotyczące sposobu postępowania z incydentem.
2. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi analizy i statystyki incydentów.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

**§ 8.**
**Gromadzenie materiału dowodowego**

1. Na każdym etapie postępowania z incydentem, dyrektor komórki właściwej ds. bezpieczeństwa informacji nadzoruje prawidłowość gromadzenia materiału dowodowego.
2. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.
3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:
   1) dla dokumentów papierowych - oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu;
   2) dla zapisów utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie (np. poza siedzibą Agencji).
4. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w załączniku nr 1 do niniejszego regulaminu.
5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w załączniku nr 2 do niniejszego regulaminu.
6. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z incydentem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

**Załącznik nr 1 do Regulaminu zarządzania incydentami - Instrukcja zabezpieczania komputerów**

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, NIE WŁĄCZAJ GO.
3. Jeśli urządzenie jest włączone, NIE próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotuj wszystkie parametry połączeń komputera:
   1) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   2) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
   3) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
4. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
5. Następnie ODŁĄCZ WSZYSTIE KABLE ZEWNĘTRZNE KOMPUTERA. Zanotuj czas odłączenia kabli.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych. ZAPLOMBUJ WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Agencję albo opis jego indywidualnych cech. Wpisz do PROTOKOŁU wykonane czynności (Załącznik nr 2 do Regulaminu zarządzania incydentami).
7. Pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp.).
8. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (dyskietki, płyty CD itp.). PAKUJ, NUMERUJ poszczególne paczki, PLOMBUJ I OPISZ W PROTOKOLE. Wpisz do PROTOKOŁU wykonane czynności.
9. Zażądaj od użytkownika spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem - okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli użytkownik nie ma spisu oprogramowania, to zażądaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokółu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.
10. Zażądaj od użytkownika przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych (np. FK). Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do BIOS-u, systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejęcia parametrów dostępu do protokołu.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.

Uwagi końcowe:

a) Sprawdź przed odesłaniem zgodność numerów zabezpieczonych materiałów i dowodów z treścią protokołu (zwróć uwagę na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach),
b) Skontaktuj się z odpowiednią komórką organizacyjną Agencji w celu zorganizowania przewozu i badań zabezpieczonych materiałów.

PAMIĘTAJ:

NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI NOŚNIKÓW DANYCH.

KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.

**Załącznik nr 2 do Regulaminu zarządzania incydentami - Wzór protokołu zabezpieczenia materiału dowodowego**

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>
Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>
Świadek 3: <imię i nazwisko, niezależny ekspert>

## I. Rodzaj materiału dowodowego

*(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)*

| | | | | | |
|---|---|---|---|---|---|
| Dokument papierowy | ☐ | *Rodzaj i Nazwa dokumentu:* ..... | | | |
| Dokument elektroniczny | ☐ | *Rodzaj i Nazwa dokumentu:* ..... | | | |
| Kopia zapasowa | ☐ | System operacyjny *Nazwa i wersja systemu:* ..... | | Aplikacja *Nazwa i wersja aplikacji:* ..... | ☐ |
| | | Baza danych *Nazwa i wersja bazy*: ..... | ☐ | Oznaczenie nośnika ..... | |
| Obraz dysku | ☐ | Lokalizacja dysku (adres IP/IPX): ..... Typ i nr seryjny dysku: ..... | | | |
| Pliki konfiguracyjne i/lub systemowe | ☐ | System operacyjny *Nazwa i wersja systemu:* ..... | ☐ | Aplikacja *Nazwa i wersja aplikacji:* ..... | ☐ |
| | | Baza danych *Nazwa i wersja bazy*: ..... | ☐ | Nazwa(y) Pliku(ów) ..... ..... ..... | |
| Kopie zawartości dzienników (logów) zdarzeń ..... | ☐ | System operacyjny *Nazwa i wersja systemu:* ..... | ☐ | Aplikacja *Nazwa i wersja aplikacji:* ..... | ☐ |
| | | Baza danych *Nazwa i wersja bazy*: ..... | ☐ | Nazwa(y) Pliku(ów) ..... ..... ..... | |
| Kopia zawartości skrzynki pocztowej | ☐ | zewnętrzna | ☐ | wewnętrzna | ☐ |
| | | *Nazwa skrzynki pocztowej:* ..... | | *Za okres od:* ..... | |

## II. Opis czynności

*(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów)*)

## III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:
„....., Egzemplarz nr 1”
„....., Egzemplarz nr 2”
*(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)*

## IV. Zabezpieczenie materiału dowodowego

*(opisać sposób zabezpieczenia jednego z egzemplarzy)*

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

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

Protokół sporządził: .....

Podpisano:

Świadek 1 . . . . . .
Świadek 2 . . . . . .
Świadek 3 . . . . . .

**Załącznik nr 3 do Regulaminu zarządzania incydentami - Wzór raportu z incydentu**

*Miejscowość, data*

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

A. ZGŁOSZENIE INCYDENTU (wypełnia osoba zgłaszająca zdarzenie/incydent)

DANE OSOBY ZGŁASZAJĄCEJ

Imię i nazwisko……Stanowisko służbowe …….
Adres ……..
Nr telefonu ……e-mail …….

OPIS INCYDENTU:

……...……..……
……
……
……
……
……..……
……
……
……
……
……

Komu zgłoszono: …….

Data i godzina zgłoszenia: …….

Podpis osoby zgłaszającej ……

B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU

(wypełnia osoba rozpatrująca zgłoszenie incydentu)
*DANE OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU - ADMINISTRATOR SYSTEMU/ ADMINISTRATOR ZABEZPIECZEŃ FIZYCZNYCH/ IBI*

Imię i nazwisko……... Stanowisko ……
Adres ……
Nr telefonu …… e-mail ……

INFORMACJE O INCYDENCIE

Data i czas zajścia incydentu ……
Data i czas wykrycia incydentu ……
Data i czas zgłoszenia incydentu ……
Czy incydent jest zakończony? TAK ☐ NIE ☐
Jeśli tak, to jak długo trwał (dni/godziny/minuty)? ……
Jeśli nie, należy określić jak długo już trwa?……
Kogo powiadomiono z KIEROWNICTWA? ……

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO

……
……
……
……
……

Załączniki (materiał dowodowy):
1. …….
2. …….
3. …….

OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA

……
……
……
……

Imię i Nazwisko …….
Data ……
Podpis ……

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE INCYDENTU

(wypełnia osoba prowadząca postępowanie wyjaśniające – IBI w Centrali/OR)

Data rozpoczęcia postępowania ws. incydentu ……
Data zakończenia incydentu (jeśli jest zakończony) ……
Data zamknięcia skutków incydentu ……
Data zakończenia postępowania ws. incydentu ……
Data przedstawienia incydentu na KSBI ……

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU
(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

……
……
……
……
……

WNIOSKI I REKOMENDACJE
(w tym zalecenia dotyczące zmian w SZBI)

……
……
……
……
……
……

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

……
……
……

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko ……. Imię i Nazwisko ……

Stanowisko ……. Stanowisko ……

Data ……. Data ……..

Podpis …… Podpis ……

**REGULAMIN OCHRONY DANYCH OSOBOWYCH**

**Spis treści:**

**Rozdział 1**
**Definicje**

**§ 1.**

Użyte w regulaminie określenia oznaczają:

1) Administrator danych – Agencja Restrukturyzacji i Modernizacji Rolnictwa;
2) UODO – Urząd Ochrony Danych Osobowych;
3) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
4) RODO - Rozporządzenie Parlamentu Europejskiego 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);
5) Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
6) Inspektor Ochrony Danych (IOD) – wyznaczony przez Administratora danych pracownik realizujący zadania, o których mowa w art. 39 RODO;
7) Właściciel zbioru – dyrektor komórki organizacyjnej w Centrali Agencji, któremu powierzono zbiór danych osobowych;
8) Współadministrator – administrator, który wspólnie z innym lub innymi administratorami ustala cele i sposoby przetwarzania. W drodze wspólnych uzgodnień współadministratorzy określają zakres swojej odpowiedzialności, dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba, że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo krajowe, któremu administratorzy ci podlegają;
9) Przedstawiciel administratora – osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora na mocy art. 27 do reprezentowania administratora w zakresie jego obowiązków wynikających z RODO;
10) Podmiot przetwarzający – podmiot przetwarzający dane osobowe na podstawie umowy lub innego instrumentu prawnego w imieniu Administratora danych, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób których dane dotyczą;
11) Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
12) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych;
13) Privacy by design – zasady ochrony danych osobowych na etapie projektowania systemu służącego do przetwarzania danych osobowych;
14) Privacy by default – zasady ochrony danych osobowych w zakresie podstawowym (domyślne);
15) Privacy Impact Assessment – ocena skutków dla ochrony danych osobowych;
16) Osoba, której dane dotyczą – każda osoba fizyczna, których dane są przetwarzane przez Administratora danych;
17) Prawa osób, których dane dotyczą – prawa, o których mowa w art. 15-21 RODO;
18) Nowy Projekt – każda nowa inicjatywa, której realizacja będzie wiązać się z przetwarzaniem danych osobowych. Nowym projektem będzie w szczególności: zorganizowanie konkursu, stworzenie nowej lub modyfikacja istniejącej aplikacji, wdrożenie nowej lub modyfikacja istniejącej usługi, jeśli w ramach jej świadczenia będzie dochodzić do przetwarzania danych, lub wdrożenie nowego procesu przetwarzania danych osobowych.

**Rozdział 2**
**Cel przetwarzania danych osobowych**

**§ 2.**

1. Agencja przetwarza dane osobowe w celu realizacji zadań określonych w ustawie o Agencji Restrukturyzacji i Modernizacji Rolnictwa oraz w związku z wykonywaniem innych ustaw.
2. Dane osobowe są przetwarzane do czasu realizacji celu, dla którego zostały pozyskane, chyba, że przepisy innych ustaw stanowią inaczej.

3. Niniejszy regulamin ma zastosowanie do danych osobowych przetwarzanych we wszystkich zasobach Agencji, a w szczególności w systemach teleinformatycznych, poza systemami teleinformatycznymi oraz na wszelkich nośnikach danych.

## Rozdział 3
## Organizacja bezpieczeństwa

### § 3.

1. Przestrzeganie zasad ochrony danych osobowych należy do obowiązków wszystkich pracowników jednostek i komórek organizacyjnych Agencji oraz podmiotów zewnętrznych współpracujących z Agencją.
2. Właściciel zbioru wykonuje obowiązki Administratora danych wobec powierzonego mu zbioru danych osobowych za wyjątkiem tych obowiązków, które zostały przekazane innym podmiotom.
3. Właściciel zbioru jest obowiązany zapewnić ochronę przetwarzanych danych osobowych przez zastosowanie środków technicznych i organizacyjnych zapewniających ochronę odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed dostępem do nich osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, ich zmianą, utratą, uszkodzeniem lub zniszczeniem oraz zapewnić, aby dane były przetwarzane zgodnie z przepisami prawa.
4. Szczegółowe zakresy obowiązków i odpowiedzialności Właściciela Zasobu ustanowione w Polityce bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do Właściciela zbioru.
5. Właściciel zbioru nie może delegować swoich zadań do podmiotów zewnętrznych.
6. Dyrektor oddziału regionalnego nie jest Właścicielem zbioru.

### § 4.

1. Do zadań Inspektora Ochrony Danych należy:
   1) kreowanie polityki ochrony danych osobowych oraz dokonywanie jej wykładni poprzez:
      a) określanie zasad przetwarzania danych osobowych m.in. ich udostępniania i powierzania, a także zasad ochrony danych osobowych i zarządzania danymi osobowymi,
      b) określenie jednolitego dla całej Agencji sposobu prowadzenia dokumentacji, o której mowa w RODO oraz dokumentowania wykonania czynności wymaganych w RODO,
      c) sporządzanie i przedstawianie stanowiska w sprawie stosowania obowiązującego w tym zakresie prawa,
      d) inicjowanie, tworzenie i aktualizacja procedur oraz innych dokumentów wynikających z zadań powierzonych w polityce ochrony danych osobowych,
      e) opiniowanie, pod względem zgodności z przepisami o ochronie danych osobowych oraz polityką ochrony danych osobowych, umów (w tym umów powierzenia przewarzania danych), porozumień, procedur i innych dokumentów wytworzonych w Agencji, dotyczących bezpieczeństwa i przetwarzania danych osobowych,
      f) wspieranie dyrektora komórki ds. bezpieczeństwa w zakresie opiniowania nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by defoult);
   2) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz polityki ochrony danych osobowych, w szczególności poprzez:
      a) zbieranie informacji w celu identyfikacji procesów przetwarzania,
      b) zbieranie informacji w celu zapewnienia przestrzegania polityki ochrony danych osobowych,
      c) nadzorowanie i koordynowanie prowadzenia przez Właścicieli zbiorów rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania,
      d) prowadzenie zbiorczych rejestrów czynności przetwarzania oraz zbiorczych rejestrów kategorii czynności przetwarzania,
      e) prowadzenie zbiorczego rejestru umów powierzenia na podstawie danych przekazywanych przez Właścicieli zbiorów,
      f) wykonywanie czynności audytowych weryfikujących zgodność przetwarzania danych oraz rekomendowanie określonych działań w tym zakresie. Realizując uprawnienie, o którym mowa w zdaniu pierwszym Inspektor Ochrony Danych w szczególności:
         – audytuje sposób przetwarzania danych osobowych we wszystkich komórkach i jednostkach organizacyjnych Agencji,
         – audytuje sposób przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych we wszystkich komórkach i jednostkach organizacyjnych Agencji,

g) wydawanie zaleceń Właścicielom zbiorów, dyrektorom oddziałów regionalnych i innym osobom odpowiedzialnym za ochronę i zgodne z prawem przetwarzanie danych osobowych w Agencji;

3) zwiększanie świadomości personelu uczestniczącego w operacjach przetwarzania danych osobowych, poprzez prowadzenie szkoleń (z wyjątkiem szkoleń podstawowych dla osób nowozatrudnionych) i udzielanie konsultacji w zakresie ochrony danych osobowych;

4) udzielanie na żądanie Właściciela zbioru/dyrektora oddziału regionalnego zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 RODO. Dokonując oceny Właściciel zbioru/dyrektor oddziału regionalnego może konsultować z Inspektorem Ochrony Danych m.in. następujące kwestie:

a) czy zasadne jest przeprowadzenie oceny skutków dla ochrony danych,

b) metodologię przeprowadzania oceny skutków dla ochrony danych,

c) czy zasadne jest przeprowadzenie wewnętrznej oceny czy zlecenie jej podmiotowi zewnętrznemu,

d) zabezpieczenia (w tym środki techniczne i organizacyjne) stosowane do minimalizowania wszelkich zagrożeń praw i interesów osób, których dane dotyczą,

e) prawidłowości przeprowadzenia oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie oraz jakie zabezpieczenia należy zastosować);

5) współpraca z PUODO (organem nadzorczym) w kwestiach związanych z przetwarzaniem danych osobowych, w tym reprezentowanie Administratora danych w postępowaniach skargowych prowadzonych przed PUODO;

6) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami związanymi z dokonywaniem oceny skutków dla ochrony danych, o których mowa w art. 36 RODO, oraz – w stosownych przypadkach – prowadzenie konsultacji we wszelkich innych sprawach;

7) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą;

8) ocena, czy istnieje w danym stanie faktycznym wymóg zgłaszania naruszenia ochrony danych osobowych;

9) ocena, czy istnieje w danym stanie faktycznym wymóg zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych;

10) prowadzenie rejestru naruszeń ochrony danych osobowych.

2. Osoby zatrudnione w ARiMR na podstawie umowy o pracę oraz osoby wykonujące pracę na podstawie innych form zatrudnienia, a także stażyści, praktykanci i wolontariusze mają obowiązek współpracy z Inspektorem Ochrony Danych, w związku z realizacją jego zadań, a także niezwłocznego informowania, w szczególności o incydentach lub podejrzeniach incydentów związanych z ochroną danych osobowych, w tym naruszeniach ochrony danych.

3. Każdy zbiór danych osobowych przetwarzanych w Agencji posiada Właściciela zbioru ustanowionego w formie zarządzenia.

4. Właściciel zbioru odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności odpowiada za:

1) przetwarzanie danych osobowych zgodne z zasadami określonymi w art. 5 RODO, tj.:

a) zasadą legalności, rzetelności i przejrzystości danych – przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Właściciel zbioru zapewnia przejrzystość przetwarzania danych, w szczególności poprzez informowanie osób, których dane dotyczą o przetwarzaniu danych z chwilą ich pozyskania, w tym o celu i podstawie prawnej przetwarzania. Właściciel zbioru zapewnia, aby dane były zbierane tylko w zakresie niezbędnym do wskazanego celu i przetwarzane tylko przez okres, w jakim jest to niezbędne,

b) zasadą celowości (ograniczenia celu) – dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) zasadą adekwatności (minimalizacji danych) – dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

d) zasadą merytorycznej poprawności (prawidłowości danych) – dane osobowe powinny być merytorycznie poprawne, a ich zakres i rodzaj adekwatny do celu, w jakim są przetwarzane, oraz w razie potrzeby uaktualniane. Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania powinny zaś zostać niezwłocznie usunięte lub sprostowane,

e) zasadą ograniczenia czasowego (ograniczenia przechowywania) – dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Właściciel zbioru po osiągnięciu celów przetwarzania danych powinien usunąć te dane albo je zanonimizować,

f) zasadą zabezpieczenia danych (integralności i poufności danych) – dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

Zasady, o których mowa w pkt 1 lit. a – f powinny być spełnione łącznie, a Właściciel zbioru jest odpowiedzialny za ich przestrzeganie. Mając na względzie „zasadę rozliczalności", o której mowa w ust. 2 art. 5 RODO, Właściciel zbioru powinien być w stanie wykazać ich przestrzeganie;

2) prowadzenie w formie papierowej lub w formie elektronicznej rejestru czynności przetwarzania danych osobowych, którego jest właścicielem, zawierającego:

a) nazwę oraz dane kontaktowe Administratora danych oraz wszelkich współadministratorów, a także Inspektora Ochrony Danych,

b) cele przetwarzania,

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa adekwatnych do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony danych;

3) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane i/lub udostępniane;

4) nadawanie upoważnień do przetwarzania danych osobowych;

5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

6) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w oparciu o szacowanie ryzyka;

7) nadzorowanie systemów teleinformatycznych służących do przetwarzania powierzonych zbiorów danych osobowych za pośrednictwem Administratora Systemu;

8) terminowe przekazywanie dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych – informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;

9) zapewnienie warunków i pomocy osobom dokonującym kontroli, o której mowa w § 22 ust. 1;

10) przed przystąpieniem do przetwarzania danych dokonanie analizy ryzyka, a w przypadku stwierdzenia występowania wysokiego ryzyka, przeprowadzenie oceny skutków dla ochrony danych, przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania oraz źródła ryzyka;

11) obsługę wniosków osób, których dane dotyczą związanych z realizacją ich praw, w zakresie przetwarzania ich danych osobowych;

12) prowadzenie rejestru wniosków osób, których dane dotyczą, związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych.

5. W przypadku, gdy Właściciel zbioru występuje w roli podmiotu przetwarzającego zobowiązany jest do prowadzenia w formie papierowej lub w formie elektronicznej rejestru kategorii czynności przetwarzania danych osobowych, którego jest właścicielem, zawierającego:

1) nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora oraz Inspektora Ochrony Danych,

2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

3) gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa adekwatnych do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony danych.

**§ 5.**

Administrator Systemu jest odpowiedzialny za utrzymanie i bezpieczeństwo systemów teleinformatycznych służących do przetwarzania danych osobowych.

**§ 6.**

1. Dyrektor oddziału regionalnego ponosi odpowiedzialność za stosowanie w oddziale regionalnym i podległych biurach powiatowych obowiązujących środków technicznych i organizacyjnych, niezbędnych do zapewnienia odpowiedniej ochrony danych osobowych, oraz przetwarzanie tych danych na zasadach określonych w § 5 ust. 2 pkt 1.
2. Obowiązki Właściciela zasobu i przypisana mu odpowiedzialność, ustanowione w Polityce bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do dyrektora oddziału regionalnego administrującego w oddziale regionalnym zbiorami danych osobowych.
3. Dyrektor oddziału regionalnego jest zobowiązany w szczególności do:
   1) nadawania upoważnień do przetwarzania danych osobowych i prowadzenia ewidencji osób upoważnionych;
   2) rozpatrywania wniosków o udostępnienie danych;
   3) zawierania umów powierzenia przetwarzania danych realizowanych w oddziale regionalnym;
   4) terminowego przekazywania dyrektorowi komórki właściwej ds. bezpieczeństwa informacji oraz Inspektorowi Ochrony Danych - informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;
   5) zapewnienia warunków i pomocy osobom dokonującym audytu w oddziale regionalnym i podległych biurach powiatowych;
   6) obsługi wniosków osób, których dane dotyczą związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych.

**§ 7.**

Do obowiązków Inspektora Bezpieczeństwa Informacji w OR należy w szczególności:

1) rozpatrywanie wniosków o udostępnienie danych osobowych;
2) dokonywanie wpisów w ewidencji udostępnień danych osobowych w systemie teleinformatycznym;
3) przechowywanie i aktualizacja wykazu umów powierzenia przetwarzania danych osobowych;
4) przechowywanie aktualnego wykazu osób wyznaczonych do rozpatrywania wniosków o udostępnianie danych osobowych w biurach powiatowych oraz dokumentacji szkoleń przeprowadzonych dla tych osób zawierającej m.in. prezentację na szkolenie i listy obecności uczestników;
5) przechowywanie dokumentacji szkoleń, o których mowa w § 15 ust. 4 przeprowadzonych dla kierowników biur powiatowych, zawierającej m.in. prezentację na szkolenie i listy obecności uczestników.

**§ 8.**

1. Dyrektor komórki ds. bezpieczeństwa nadzoruje przestrzeganie w Agencji polityki ochrony danych osobowych, w tym stosowanie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.
2. Nadzorowanie przestrzegania polityki ochrony danych osobowych następuje m.in. przez wykonywanie czynności audytowych, wydawanie wiążących poleceń Właścicielom zbiorów, dyrektorom oddziałów regionalnych i innym osobom odpowiedzialnym za ochronę i zgodne z prawem przetwarzanie danych osobowych w Agencji oraz poprzez sporządzanie pisemnych wystąpień w tym zakresie.
3. Wyznaczone zadania w zakresie nadzoru nad przestrzeganiem polityki ochrony danych osobowych w Agencji wykonują Inspektorzy Bezpieczeństwa Informacji z Centrali. Inspektorzy Bezpieczeństwa Informacji z Centrali wykonują zadania m.in. w zakresie:
   1) opiniowania, pod względem zgodności z przepisami o ochronie danych osobowych oraz polityką ochrony danych osobowych, umów (w tym umów powierzenia przewarzania danych), porozumień, dokumentów wewnętrznych oraz aktów prawnych wewnętrznych i zewnętrznych;
   2) opiniowania nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by defoult);
   3) audytowania sposobu przetwarzania danych osobowych w Agencji;

4) audytowania sposobu przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji;

5) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w Agencji.

4. Bieżący nadzór nad przestrzeganiem polityki ochrony danych osobowych w oddziale regionalnym i podległych biurach powiatowych wykonuje dyrektor oddziału regionalnego za pośrednictwem Inspektorów Bezpieczeństwa Informacji w oddziale regionalnym. Inspektorzy Bezpieczeństwa Informacji w oddziale regionalnym wykonują m.in. zadania w zakresie:

1) prowadzenia przeglądów w zakresie przetwarzania danych osobowych w oddziale regionalnym i biurach powiatowych;

2) prowadzenia przeglądów w zakresie przestrzegania w oddziale regionalnym i biurach powiatowych obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji;

3) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w oddziale regionalnym i biurach powiatowych;

4) opiniowanie nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by defoult).

5. Dyrektor komórki ds. bezpieczeństwa może wyznaczać dyrektorowi oddziału regionalnego zadania i żądać wyjaśnień w tym zakresie, wydawać polecenia, a także żądać informacji i opinii dotyczących przestrzegania polityki ochrony danych osobowych.

6. Upoważnienie do realizacji czynności audytowych/przeglądów Inspektorom Bezpieczeństwa Informacji w Centrali/oddziale regionalnym wydaje odpowiednio:

1) Prezes ARiMR;

2) dyrektor oddziału regionalnego.

## Rozdział 4

## Prowadzenie dokumentacji w zakresie bezpieczeństwa danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

### § 9.

1. Obszar przetwarzania danych osobowych w Agencji stanowi wykaz adresów obiektów:

1) w których są przetwarzane dane osobowe przez Agencję;

2) stanowiących lokalizację Równoległego Ośrodka Przetwarzania Danych;

3) stanowiących lokalizację Centrum Przetwarzania Danych.

2. Wykaz adresów obiektów stanowiących obszar przetwarzania danych osobowych na druku stanowiącym załącznik nr 1 do niniejszego regulaminu, w terminie do dnia 31 grudnia każdego roku kalendarzowego, dostarcza dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych:

1) Administrator Zabezpieczeń Fizycznych w Centrali Agencji – w odniesieniu do obiektów (budynków) Centrali, oddziałów regionalnych i biur powiatowych,

2) Administrator Systemu - w odniesieniu do Centrum Przetwarzania Danych i Równoległego Ośrodka Przetwarzania Danych.

3. Osoby wymienione w ust. 2 pkt 1 i 2 informują dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących lokalizacji obszarów przetwarzania w terminie 7 dni od wystąpienia zmiany.

4. Administrator Systemu sporządza:

1) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

2) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, który może być sporządzony w wersji elektronicznej;

3) informację o sposobie przepływu danych pomiędzy poszczególnymi systemami;

4) opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

5. Środki techniczne i organizacyjne dobierane są adekwatnie do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony.
6. Administrator Systemu aktualizuje informacje, o których mowa w ust. 4 pkt 1 – 4 w terminie 7 dni od wystąpienia zmian i przesyła aktualne wersje dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych.

**§ 10.**

1. Dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zawiera opis sposobu realizacji wymogów dotyczących ochrony danych osobowych.
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz regulaminy z nią powiązane i procedury w niej wskazane opracowuje i aktualizuje Administrator Systemu.
3. Administrator Systemu w terminie 7 dni od wystąpienia zmiany, przesyła dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych aktualną wersję Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Administrator Systemu zapewnia domyślną ochronę systemów teleinformatycznych służących do przetwarzania danych osobowych.
5. Właściciel zbioru nadzoruje Administratora Systemu w zakresie zapewnienia wymaganych funkcjonalności dla systemów teleinformatycznych służących do przetwarzania zbiorów danych osobowych.
6. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych określa regulamin zarządzania incydentami bezpieczeństwa informacji.

## Rozdział 5
## Tworzenie i usuwanie zbiorów danych osobowych

**§ 11.**

1. Właściciel zbioru zobowiązany jest zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o utworzeniu nowego zbioru nie później niż w terminie 7 dni od rozpoczęcia tworzenia zbioru.
2. Zawiadomienie następuje przez przesłanie informacji w zakresie:
   1) nazwy zbioru danych osobowych;
   2) podstawy prawnej przetwarzania;
   3) celu przetwarzania;
   4) opisu kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   5) kategorii odbiorców, którym dane osobowe zostaną ujawnione, w tym odbiorców państw trzecich lub w organizacjach międzynarodowych;
   6) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
   7) planowanych terminów usunięcia poszczególnych kategorii danych;
   8) ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO uwzględniających ryzyko przetwarzania danych w zgłaszanym zbiorze.
3. Na wniosek Właściciela zbioru, w przypadku tworzenia nowego zbioru Administrator Systemu określa warunki techniczne dotyczące zabezpieczeń zbioru w systemie teleinformatycznym.
4. Właściciel zbioru jest zobowiązany zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących przetwarzania danych osobowych w zbiorze nie później niż w terminie 14 dni od ich wystąpienia.
5. Administrator Systemu jest zobowiązany zgłosić Właścicielowi zbioru wszelkie zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczenia w systemie teleinformatycznym w ciągu 7 dni od daty zaistnienia tych zmian.

**§ 12.**

1. W przypadku zaprzestania przetwarzania danych w zbiorze Właściciel Zbioru jest zobowiązany niezwłocznie poinformować dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o tym fakcie. Informacja, o której mowa w zdaniu pierwszym powinna zawierać uzasadnienie.

2. Właściciel zbioru decyduje o trwałym usunięciu zbioru danych osobowych. O tym fakcie informuje dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych. W razie wątpliwości, przed usunięciem zbioru danych osobowych Właściciel zbioru zasięga opinii Inspektora Ochrony Danych.
3. Właściciel zbioru podejmuje działania w celu usunięcia zbioru danych osobowych ze wszystkich nośników.
4. Zbiory danych osobowych są likwidowane komisyjnie.
5. W skład komisji powołanej przez Administratora danych wchodzą:
   1) Administrator Systemu, jeżeli zbiór jest przetwarzany w systemie informatycznym;
   2) dwie osoby reprezentujące Właściciela zbioru.
6. Właściciel Zbioru przekazuje dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych kopię protokołu komisyjnie zlikwidowanego zbioru.

## Rozdział 6
## Nadawanie, zmiana i odbieranie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych

### § 13.

1. Przetwarzanie danych osobowych w Agencji wymaga uzyskania upoważnienia do przetwarzania danych osobowych.
2. Upoważnienie nadaje się przed dopuszczeniem osoby do przetwarzania danych osobowych.

### § 14.

1. Upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne) może być nadane:
   1) osobom przyjmowanym do pracy, bez względu na podstawę prawną zatrudnienia, po odbyciu szkolenia podstawowego;
   2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia.
2. Dyrektor komórki właściwej ds. kadrowych w Centrali/wyznaczona osoba z komórki właściwej ds. kadrowych w oddziale regionalnym/kierownik biura powiatowego w przypadku, o którym mowa w ust. 4, zapoznają osoby przyjmowane do pracy z aktami prawnymi zawierającymi przepisy o ochronie danych osobowych.
3. Inspektor Ochrony Danych publikuje na stronie internetowej Agencji w zakładce Ochrona Danych Osobowych wykaz aktów prawnych zawierających przepisy o ochronie danych osobowych.
4. Dyrektor komórki właściwej ds. kadrowych w Centrali/wyznaczona osoba z komórki właściwej ds. kadrowych w oddziale regionalnym kierują osoby przyjmowane do pracy na szkolenie podstawowe z zakresu ochrony danych osobowych i w razie potrzeby na szkolenie w zakresie przetwarzania szczególnych kategorii danych. Szkolenie prowadzi Inspektor Bezpieczeństwa Informacji odpowiedni dla jednostki organizacyjnej ARiMR, po uprzednim uzgodnieniu terminu szkolenia. W wyjątkowych przypadkach szkolenie dla stażystów, praktykantów i wolontariuszy może przeprowadzić, uprzednio przeszkolony przez Inspektora Bezpieczeństwa Informacji w OR, kierownik biura powiatowego, do którego osoby te zostały skierowane do pracy. Prezentację przeznaczoną na potrzeby szkolenia podstawowego dla kierownika BP przygotowuje Inspektor Bezpieczeństwa Informacji w OR.
5. Szkoleniu, o którym mowa w ust. 4, podlegają również:
   1) osoby zatrudnione, a niewykonujące pracy w Agencji przez okres co najmniej 12 miesięcy;
   2) osoby, które w wyniku awansu obejmują stanowisko kierownika komórki organizacyjnej albo kierownika jednostki organizacyjnej lub jego zastępcy.
6. Fakt przeprowadzenia szkolenia jest dokumentowany przez sporządzenie listy obecności uczestników. Listę obecności sporządza się na druku stanowiącym załącznik nr 3 do Regulaminu bezpieczeństwa informacji w zarządzaniu zasobami ludzkimi (załącznik nr 10 do Polityki).
7. Dyrektor komórki właściwej ds. bezpieczeństwa zawiadamia dyrektora komórki właściwej ds. kadrowych w Centrali oraz odpowiednio Inspektora Bezpieczeństwa Informacji w OR - komórkę właściwą ds. kadrowych w oddziale regionalnym, o osobach uczestniczących w szkoleniu podstawowym w zakresie bezpieczeństwa informacji. Zawiadomienie następuje przez doręczenie listy obecności uczestników. Osoby, które nie odbyły szkolenia podstawowego nie mogą zostać dopuszczone do pracy związanej z przetwarzaniem danych osobowych.

8. Osoba przeszkolona potwierdza uczestnictwo w szkoleniu, zapoznanie się z przepisami o ochronie danych osobowych i zobowiązuje się do zachowania w poufności przetwarzanych danych i innych informacji prawnie chronionych oraz zastosowanych w Agencji środków ochrony.
9. Treść oświadczenia zamieszczona jest na druku stanowiącym załącznik nr 2 do niniejszego regulaminu. Dokument po wypełnieniu dołącza się do akt osobowych lub podobnych akt prowadzonych dla osób wykonujących pracę w Agencji na innej podstawie niż stosunek pracy.
10. Kopie list obecności uczestników szkoleń podstawowych przeprowadzanych przez kierowników biur powiatowych oraz oryginały dokumentów zawierających oświadczenie przesyłane są do Inspektora Bezpieczeństwa Informacji w OR. Kopie list obecności z BP przechowywane są przez Inspektora Bezpieczeństwa Informacji w OR i składają się na prowadzoną przez niego ewidencję szkoleń. Oryginały dokumentów zawierających oświadczenie otrzymane z BP są niezwłocznie przekazywane do komórki właściwej ds. kadrowych w OR. Kierownik biura powiatowego wysyła wymienione dokumenty najpóźniej w dniu roboczym następującym po dniu jego sporządzenia.
11. Upoważnienie do przetwarzania danych osobowych w Centrali, osobom wskazanym w ust. 1 nadaje dyrektor komórki właściwej ds. kadrowych oraz odpowiednio w oddziale regionalnym i biurach powiatowych - dyrektor oddziału regionalnego, wypełniając druk stanowiący załącznik nr 2 do niniejszego regulaminu. Dyrektorom wszystkich komórek organizacyjnych w Centrali oraz dyrektorom oddziałów regionalnych i zastępcom dyrektora upoważnienie nadaje Prezes Agencji lub osoba przez niego upoważniona. Upoważnienie przechowuje się w aktach osobowych lub aktach prowadzonych dla osób zatrudnionych na podstawie innej formy zatrudnienia niż umowa o pracę.
12. W szczególnie uzasadnionych przypadkach, dyrektor komórki właściwej ds. kadrowych w Centrali/dyrektor oddziału regionalnego mogą nadać upoważnienie osobom wskazanym w ust. 1 pkt 2 bez ich przeszkolenia, równocześnie wskazując obowiązek odbycia ww. szkolenia w terminie nie przekraczającym jednego miesiąca od nadania upoważnienia.
13. Dyrektor komórki właściwej ds. kadrowych oraz dyrektor oddziału regionalnego w komórce właściwej ds. kadrowych prowadzą w formie elektronicznej, z zachowaniem chronologii, wykaz osób, którym nadano upoważnienia, wg wzoru stanowiącego załącznik nr 3 do niniejszego regulaminu. Wykaz składa się na ewidencję osób upoważnionych.
14. Upoważnienie do przetwarzania danych osobowych, bez obowiązku uczestniczenia w szkoleniu podstawowym z zakresu ochrony danych osobowych, z dniem zatrudnienia nabywają:
    1) Prezes ARiMR;
    2) Zastępcy Prezesa.
15. Osoby, o których mowa w ust. 14, podpisują oświadczenie na druku upoważnienia, którego wzór stanowi załącznik nr 2 do niniejszego regulaminu, przekazanym przez dyrektora komórki właściwej ds. kadrowych, w którym zobowiązują się do zachowania w tajemnicy/poufności przetwarzanych danych oraz zastosowanych w Agencji środków ochrony.
16. Oświadczenie o którym mowa w ust. 15 przechowywane jest w ich aktach osobowych.

**§ 15.**

1. Upoważnienie do przetwarzania danych w zbiorach (upoważnienie szczególne) może być nadane:
    1) osobom zatrudnionym (wykonującym pracę) w Agencji bez względu na podstawę prawną zatrudnienia, jeżeli uzyskały one upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne);
    2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia; osobom tym można nadać upoważnienie bez obowiązku uprzedniego uzyskania upoważnienia ogólnego.
2. Upoważnienie do przetwarzania danych w zbiorach przetwarzanych w systemie informatycznym jest nadawane w wyniku zaakceptowania przez Właściciela zbioru wniosku o nadanie uprawnień do pracy w systemie. Druk wniosku określono w Książce procedur KP-611-101-ARiMR „Obsługa kont użytkowników systemów informatycznych ARiMR".
3. Wobec zbiorów przetwarzanych w systemie informatycznym w Centrali Agencji, z wnioskiem o nadanie uprawnień do pracy w systemie występują osoby określone w KP-611-101-ARiMR.
4. Wniosek o nadanie uprawnień do pracy w systemie jest zatwierdzany przez wszystkich Właścicieli zbiorów, do których zbiorów danych osobowych będzie miała dostęp osoba, której zostaną nadane uprawnienia, z zastrzeżeniem ust. 7.
5. Wniosek o nadanie uprawnień po uprzednim zatwierdzeniu przez Właściciela(i) zbioru(ów), realizuje Administrator Systemu.
6. Zbiór wszystkich zrealizowanych wniosków o nadanie uprawnień do pracy w systemie informatycznym, przechowywany przez Administratora Systemu, jest częścią ewidencji osób upoważnionych.

7. Wobec zbiorów przetwarzanych w systemie informatycznym w oddziałach regionalnych i biurach powiatowych Agencji wniosek o nadanie uprawnień do pracy w systemie, w mieniu Właścicieli zbiorów, zatwierdza dyrektor oddziału regionalnego.
8. Wniosek o nadanie uprawnień zatwierdzony przez dyrektora oddziału regionalnego lub osobę przez niego upoważnioną jest przechowywany w oddziale regionalnym w dokumentacji pracowniczej osoby uprawnionej.
9. Zbiór wszystkich wniosków zrealizowanych w oddziale regionalnym o nadanie uprawnień do pracy w systemie, przechowywany w oddziale regionalnym, jest częścią ewidencji osób upoważnionych.
10. Upoważnienie do przetwarzania danych osobowych w zbiorach przetwarzanych wyłącznie w formie papierowej nadają:
    1) w Centrali Agencji – Właściciel zbioru;
    2) w oddziale regionalnym i biurze powiatowym – dyrektor oddziału regionalnego.
11. Upoważnienie, o którym mowa w ust. 10 nadawane jest poprzez zatwierdzenie wniosku sporządzonego na druku stanowiącym załącznik nr 4 do niniejszego Regulaminu.
12. Do sporządzania wniosku, o którym mowa w ust. 10, stosuje się odpowiednio zasady kompetencyjne obowiązujące przy sporządzaniu wniosku o nadanie uprawnień do przetwarzania danych w systemie informatycznym.
13. Zatwierdzone wnioski o nadanie upoważnienia do przetwarzania danych w zbiorach przetwarzanych wyłącznie w formie papierowej są przechowywane odpowiednio przez Właścicieli zbiorów w Centrali Agencji i przez dyrektorów oddziałów regionalnych. Są one częścią ewidencji osób upoważnionych.

**§ 16.**

1. Zmiany upoważnienia do przetwarzania danych osobowych dokonują osoby uprawnione do jego nadawania.
2. Utrata upoważnienia do przetwarzania danych osobowych w zbiorach następuje w wyniku jego odebrania przez osobę uprawnioną. Dokument dotyczący odebrania uprawnienia przechowuje się u właściciela zasobu i w dokumentacji pracowniczej osoby.
3. Ważność upoważnienia ogólnego wygasa z chwilą zakończenia zatrudnienia.
4. Osobę uprawnioną mogą wskazywać przepisy niniejszego regulaminu lub innych regulaminów ustanowionych w ramach SZBI, a w szczególności Regulaminu bezpieczeństwa w zarządzaniu zasobami ludzkimi.

## Rozdział 7
## Ewidencja osób upoważnionych do przetwarzania danych osobowych

**§ 17.**

1. W Agencji prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Agencji zawiera łącznie:
    1) zbiór osób, które uzyskały upoważnienia do przetwarzania danych osobowych, do którego należą:
        a) osoby, których wykaz jest prowadzony w formie elektronicznej przez dyrektora komórki właściwej ds. kadrowych w Centrali oraz dyrektorów oddziałów regionalnych,
        b) Prezes i Zastępcy Prezesa;
    2) zbiór osób, które uzyskały upoważnienia do przetwarzania danych w zbiorach:
        a) przetwarzanych w systemie informatycznym,
        b) przetwarzanych wyłącznie w formie papierowej;
    3) zbiór osób, które uzyskały upoważnienia do przetwarzania danych w Agencji na mocy przepisów wcześniej obowiązujących.
3. Administrator Systemu prowadzi ewidencję identyfikatorów użytkowników systemu informatycznego, w którym są przetwarzane dane osobowe.

## Rozdział 8
## Realizacja praw osób, których dane dotyczą

**§ 18.**

1. Każdej osobie przysługuje prawo dostępu do danych osobowych, które jej dotyczą oraz do wydania kopii danych, sprostowania danych, usunięcia danych („prawo do bycia zapomnianym"), ograniczenia przetwarzania, przeniesienia danych oraz prawo do sprzeciwu, zgodnie z art. 15-21 RODO.
2. Wniosek o realizację praw osób, których dane dotyczą może być złożony w formie: pisemnej, elektronicznej (zawierającej podpis elektroniczny lub potwierdzony profil zaufany) lub osobiście. Wniosek nie może zostać odrzucony z tego względu, że został on złożony w piśmie dotyczącym innej sprawy.
3. Szczegółowe zasady w zakresie realizacji praw osób, których dane dotyczą oraz tryb postępowania z wnioskami tych osób określają „Wytyczne dotyczące realizacji praw osób, których dane dotyczą", opracowane i udostępniane, a w razie konieczności aktualizowane przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
4. Wniosek osoby, której dane dotyczą, w sprawach właściwych dla Centrali rozpatruje Właściciel zbioru. Wniosek w sprawach właściwych dla oddziału regionalnego lub biura powiatowego rozpatruje dyrektor oddziału regionalnego.
5. Inspektor Ochrony Danych udziela, w razie uzasadnionej potrzeby, niezbędnego wsparcia Właścicielowi zbioru/dyrektorowi oddziału regionalnego przy rozpatrywaniu wniosków w zakresie realizacji praw osób, których dane dotyczą.
6. Wniosek osoby, której dane dotyczą Właściciel zbioru/dyrektor oddziału regionalnego powinien rozpatrzyć bez zbędnej zwłoki, jednak w terminie nie dłuższym niż jeden miesiąc od otrzymania żądania w przedmiotowym zakresie.
7. W przypadku zamiaru przesłania odpowiedzi drogą pocztową, Właściciel zbioru/dyrektor oddziału regionalnego zapewnia, aby odpowiedź została wysłana nie później niż w terminie 3 dni roboczych przed upływem jednego miesiąca od daty otrzymania wniosku.
8. W razie potrzeby termin, o którym mowa w ust. 7, może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim przypadku, w terminie miesiąca od otrzymania żądania Właściciel zbioru/dyrektor oddziału regionalnego powinien poinformować osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
9. Właściciel zbioru/dyrektor oddziału regionalnego może odmówić podjęcia działań w związku ze złożonym wnioskiem osoby, której dane dotyczą w przypadku, gdy:
   1) wniosek jest ewidentnie nieuzasadniony;
   2) żądania osoby, której dane dotyczą są nadmierne, w szczególności, gdy ich zgłaszanie ma charakter ustawiczny.
10. O odmowie podjęcia działań, z uwagi na okoliczności, o których mowa w ust. 9 Właściciel zbioru/dyrektor oddziału regionalnego informuje osobę, której dane dotyczą w terminie miesiąca od otrzymania wniosku. Informacja udzielana jest zgodnie z wzorem formularza wniosku, określonym w załączniku do instrukcji, o której mowa w ust. 3.

## Rozdział 9
## Udostępnianie danych osobowych

### § 19.

1. Dane osobowe udostępniane są na wniosek.
2. Wniosek o udostępnienie danych osobowych, który wpłynął do biura powiatowego lub oddziału regionalnego załatwia dyrektor oddziału regionalnego.
3. Wniosek o udostępnienie danych osobowych, który z przyczyn formalnych lub merytorycznych nie może zostać załatwiony przez dyrektora oddziału regionalnego, załatwia Właściciel zbioru.
4. Wnioski o udostępnienie danych osobowych załatwiane przez dyrektora oddziału regionalnego rozpatruje Inspektor Bezpieczeństwa Informacji w OR. W tym celu m.in.:
   1) dokonuje oceny wniosków pod względem formalnym i merytorycznym;
   2) przygotowuje projekty pism w sprawie usunięcia nieprawidłowości, uzupełnienia wniosków, udzielenia niezbędnych wyjaśnień oraz projekty odpowiedzi na wnioski, które przedkłada do podpisu dyrektorowi oddziału regionalnego;
   3) występuje do komórek organizacyjnych oddziału regionalnego lub biura powiatowego o przekazanie informacji merytorycznej niezbędnej do przygotowania odpowiedzi na wnioski; za terminowość i integralność przekazanej informacji odpowiedzialność ponosi kierownik biura powiatowego lub kierownik komórki organizacyjnej oddziału regionalnego przekazujący informację.
5. Osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym opiniuje projekt pisma w sprawie usunięcia nieprawidłowości, uzupełnienia wniosku lub udzielenia niezbędnych wyjaśnień oraz projekt odpowiedzi na wniosek, jeżeli taki projekt zostanie mu przedstawiony do zaopiniowania przez

Inspektora Bezpieczeństwa Informacji w OR; akceptując projekt pisma, osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym składa na nim czytelny podpis.

6. Wniosek o udostępnienie danych osobowych z Systemu Identyfikacji i Rejestracji Zwierząt, od osoby zatrudnionej w Inspekcji Weterynaryjnej, który wpłynął do biura powiatowego załatwia kierownik biura powiatowego.
7. Kierownik biura powiatowego zgłasza do dyrektora oddziału regionalnego wykaz osób wyznaczonych do rozpatrywania wniosków o udostępnienie danych i odpowiada za jego aktualizację. Osoby te podlegają co najmniej raz w roku szkoleniom doskonalącym prowadzonym przez Inspektorów Bezpieczeństwa Informacji z OR.
8. Wniosek o udostępnienie danych osobowych załatwiany w biurze powiatowym, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany do oddziału regionalnego w celu uzyskania opinii Inspektora Bezpieczeństwa Informacji w OR. Do kopii wniosku dołącza się informacje niezbędne do jego rozpatrzenia oraz stanowisko kierownika BP.
9. Wniosek, który wpłynął do Centrali Agencji załatwia Właściciel zbioru. Wniosek organu egzekucyjnego może zostać przekazany przez Właściciela zbioru do załatwienia dyrektorowi oddziału regionalnego.
10. Właściciel zbioru jest obowiązany wyznaczyć co najmniej dwie osoby do rozpatrywania wniosków o udostępnienie danych (osoby wyznaczone), o których informuje dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych. Tylko osoby wyznaczone rozpatrują wnioski o udostępnienie danych osobowych, które załatwia Właściciel zbioru.
11. Dyrektor komórki właściwej ds. bezpieczeństwa prowadzi wykaz osób wyznaczonych, które podlegają okresowemu szkoleniu. Za przekazywanie informacji niezbędnych do prowadzenia aktualnego wykazu odpowiadają Właściciele zbiorów.
12. Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi. Projekt odpowiedzi przesłany z oddziału regionalnego wymaga podpisu osoby zatrudnionej na stanowisku radcy prawnego.
13. Dane osobowe udostępnia się na wniosek sporządzony w formie pisemnej, spełniający wymagania formalne, określone w przepisach prawa. Szczegółowe zasady postępowania przy rozpatrywaniu wniosków o udostępnienie danych osobowych określają „Wytyczne dotyczące rozpatrywania wniosków o udostępnienie danych osobowych". Obowiązujące Wytyczne są opracowywane i udostępniane, a w razie konieczności aktualizowane przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
14. Informacje zawierające dane osobowe są udostępniane uprawnionym podmiotom:
    1) w formie pisemnego wydruku, listem poleconym lub za potwierdzeniem osobistego odbioru;
    2) za pomocą elektronicznej skrzynki podawczej e-PUAP – z użyciem podpisu kwalifikowanego lub potwierdzonego profilem zaufanym;
    3) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych);
    4) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru;
    5) w inny sposób określony przepisami prawa lub umową.
15. Podstawową formą przekazywania danych osobowych jest metoda określona w ust. 14 pkt 1.
16. W szczególnie uzasadnionych przypadkach stosuje się metody określone w ust. 14 pkt 2 – 5. Uzasadnienie takiego przypadku, sporządzone na piśmie, dołącza się do akt sprawy.
17. Zawartość elektronicznych nośników informacji podlega kontroli i pisemnej akceptacji bezpośredniego przełożonego - osoby przygotowującej informację określoną w ust. 14.
18. Jeżeli tryb udostępniania danych osobowych określa umowa, przepisów niniejszego rozdziału nie stosuje się w zakresie postanowień umowy.
19. Ewidencja przypadków udostępnienia danych prowadzona jest w wyznaczonym systemie informatycznym. Ewidencję prowadzą:
    1) w Centrali Agencji – Właściciel zbioru;
    2) w oddziale regionalnym – dyrektor;
    3) w biurze powiatowym – kierownik.

## Rozdział 10
## Powierzanie przetwarzania danych osobowych innym podmiotom

**§ 20.**

1. Powierzenie przetwarzania danych nie wyłącza, ani nie ogranicza odpowiedzialności Właściciela zbioru/dyrektora oddziału regionalnego za zgodne z prawem przetwarzanie tych danych.
2. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej zgodnie z RODO.
3. Przed przekazaniem danych osobowych w ramach wykonania umowy powierzenia danych Właściciel zbioru/dyrektor oddziału regionalnego dokonuje weryfikacji czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. Ocena spełnienia przez podmiot przetwarzający wymogów, o których mowa powyżej przeprowadzana jest za pomocą ankiety. Formularz ankiety jest opracowywany, aktualizowany i udostępniany przez dyrektora komórki właściwej ds. bezpieczeństwa w sieci wewnętrznej na stronie intranetowej Agencji, przy czym wymagana jest uprzednia akceptacja w tym zakresie Inspektora Ochrony Danych.
4. Umowa powierzenia przetwarzania danych osobowych powinna zawierać elementy określone w art. 28 RODO, a zatem co najmniej:
   1) przedmiot przetwarzania (jakie dane i w jakim zakresie zostają powierzone podmiotowi przetwarzającemu);
   2) czas trwania przetwarzania;
   3) charakter i cel przetwarzania;
   4) rodzaj danych osobowych;
   5) kategorie osób, których dane dotyczą;
   6) obowiązki i prawa Administratora danych, w tym w szczególności: postanowienia określające sposób sprawowania przez Agencję kontroli należytego wykonania umowy w powyższym zakresie; postanowienia określające sposób dochodzenia roszczeń Agencji w przypadku, gdy nastąpi naruszenie ochrony danych z przyczyn leżących po stronie podmiotu, któremu powierza się ich przetwarzanie;
   7) zobowiązanie podmiotu, któremu powierza się dane osobowe do zastosowania odpowiednich środków zabezpieczających te dane, wymaganych na mocy art. 32 RODO;
   8) postanowienia dotyczące wydawania upoważnień do przetwarzania danych osobowych;
   9) zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
5. Inspektor Ochrony Danych określa wzór umowy powierzenia przetwarzania danych osobowych obowiązujący w Agencji.
6. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w Centrali Agencji, której realizacja może wiązać się z przetwarzaniem powierzonych danych osobowych Agencji, wymaga akceptacji w wyniku złożenia czytelnych podpisów przez:
   1) wszystkich Właścicieli zbiorów, których dane są powierzane;
   2) Inspektora Ochrony Danych;
   3) dyrektora komórki właściwej ds. bezpieczeństwa;
   4) Administratora Systemu.
7. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w OR Agencji, której realizacja może wiązać się z przetwarzaniem powierzonych danych osobowych, wymaga akceptacji w wyniku złożenia czytelnych podpisów przez:
   1) Dyrektora OR;
   2) kierownika komórki organizacyjnej przygotowującej projekt;
   3) Inspektora Bezpieczeństwa Informacji w OR;
   4) osoby zajmującej samodzielne stanowisko radcy prawnego w OR.
8. Właściciel zbioru nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w Centrali i wykonywanych na terenie właściwości Centrali Agencji. Dyrektor oddziału regionalnego nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w oddziale regionalnym oraz wszystkich umów wykonywanych na terenie właściwości oddziału regionalnego chyba, że Właściciel zbioru postanowi inaczej.
9. Właściciele zbiorów i dyrektorzy oddziałów regionalnych prowadzą wykaz umów powierzenia przetwarzania danych według wzoru stanowiącego załącznik nr 6 do niniejszego regulaminu.

## Rozdział 11
## Postępowanie w przypadku kontroli PUODO

### § 21.

1. PUODO lub upoważnieni przez PUODO pracownicy UODO, zwani dalej „kontrolującymi", mają prawo do przeprowadzania kontroli w Agencji. Kontrolę przeprowadza się po okazaniu przez kontrolującego imiennego upoważnienia wraz z legitymacją służbową. Imienne upoważnienie do przeprowadzania kontroli powinno zawierać elementy wskazane w art. 81 ust. 2 Ustawy.
2. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli (przedstawiciela kontrolowanej komórki lub jednostki organizacyjnej). Szczegółowe warunki i zasady przeprowadzania kontroli określa Ustawa.
3. Inspektor Ochrony Danych jest zawiadamiany bez zbędnej zwłoki o kontroli PUODO w Agencji i może być obecny podczas wykonywania przez kontrolujących czynności kontrolnych w Agencji.
4. Właściciel zbioru, Administrator Systemu, Administrator Zabezpieczeń Fizycznych, dyrektor oddziału regionalnego, kierownik biura powiatowego i inne osoby poddawane kontroli zobowiązani są do ścisłej współpracy z Inspektorem Ochrony Danych.
5. Inspektor Ochrony Danych zapewnia pod względem organizacyjnym warunki niezbędne do przeprowadzenia kontroli PUODO w Centrali Agencji.
6. Merytoryczną obsługę kontroli PUODO polegającą m.in. na udzieleniu kontrolującym niezbędnych informacji, wyjaśnień, dostępu do dokumentów i systemów teleinformatycznych w Centrali Agencji zapewniają w granicach swoich kompetencji i uprawnień:
   1) Właściciel zbioru wobec powierzonych mu zbiorów;
   2) Administrator Systemu;
   3) Administrator Zabezpieczeń Fizycznych;
   4) Inspektor Ochrony Danych;
   5) dyrektor komórki właściwej ds. bezpieczeństwa;
   6) kierownik komórki organizacyjnej, w której są przetwarzane dane osobowe;
   7) pracownicy i inne osoby wykonujące pracę na rzecz Agencji w odniesieniu do wykonywania obowiązków związanych z przetwarzaniem danych osobowych, tylko w obecności przełożonego lub osoby nadzorującej ich pracę.
7. Dyrektor oddziału regionalnego zapewnia warunki i obsługę kontroli PUODO w oddziale regionalnym.
8. Merytoryczną obsługę kontroli PUODO w oddziale regionalnym zapewniają kierownicy jednostek i komórek organizacyjnych w granicach swoich kompetencji i uprawnień. Pracownicy i inne osoby wykonujące pracę w oddziale regionalnym, związaną z przetwarzaniem danych osobowych, uczestniczą w czynnościach kontrolnych tylko w obecności przełożonego lub osoby nadzorującej ich pracę.
9. W trakcie czynności kontrolnych wykonywanych przez kontrolujących w oddziale regionalnym uczestniczy Inspektor Bezpieczeństwa Informacji z OR. Dyrektor oddziału regionalnego może wyznaczyć też inne osoby, które będą brały udział w tych czynnościach.
10. Kierownicy komórek organizacyjnych w oddziale regionalnym, kierownicy biur powiatowych i inne osoby poddawane kontroli są zobowiązane do ścisłej współpracy z Inspektorem Bezpieczeństwa Informacji w OR oraz innymi osobami wyznaczonymi przez dyrektora oddziału regionalnego.

## Rozdział 12
## Odpowiedzialność za naruszenie zasad ochrony danych osobowych

### § 22.

Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi i administracyjnymi określonymi w Ustawie oraz w Kodeksie karnym. Niezależnie od powyższego naruszenie zasad ochrony danych osobowych obowiązujących w Agencji może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną pracowników.

*Załącznik nr 1 do Regulaminu ochrony danych osobowych.*

Znak sprawy:

**Wykaz obszarów przetwarzania danych osobowych w Agencji Restrukturyzacji i Modernizacji Rolnictwa na dzień** .....

Obszary przetwarzania danych osobowych stanowi strefa administracyjna i strefa bezpieczeństwa w użytkowanych budynkach.

| Nazwa obiektu | Województwo | Powiat | Adres |
|---|---|---|---|
| | | | |

Agencja Restrukturyzacji i Modernizacji Rolnictwa
Al. Jana Pawła II 70
00-175 Warszawa
Adres do korespondencji:
ul. Poleczki 33
02-822 Warszawa
*(dane administratora)*

……., dnia…… r.
*(miejscowość, data)*

**UPOWAŻNIENIE**
**DO PRZETWARZANIA DANYCH OSOBOWYCH**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem", upoważniam:

Panią/Pana*……..,

posiadającą/ego nr. KIP* – …….., zatrudnioną/ego w ……..* Agencji Restrukturyzacji i Modernizacji Rolnictwa, do przetwarzania i polecam przetwarzanie:

- ☐ danych osobowych zwykłych;
- ☐ danych osobowych szczególnych kategorii**

w zakresie niezbędnym do wykonywania powierzonej pracy***.

Niniejsze upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w okresie wykonywania powierzonej pracy.

Jednocześnie zobowiązuje Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami Rozporządzenia, ustawy z dnia 10.05.2018 r. *o ochronie danych osobowych* (Dz. U. z 2018 r., poz. 1000 z późn.zm.), ustawy z dnia 26.06.1974 r. *Kodeks Pracy* (Dz. U. z 2018 r. poz. 917 z późn. zm.), innymi przepisami prawa powszechnie obowiązującymi, a także z przepisami wewnątrzzakładowymi ARiMR w zakresie Polityki ochrony danych osobowych Pracodawcy.

…….
*(podpis osoby uprawnionej do nadania upoważnienia)*

Oświadczam, że znane są mi przepisy z zakresu ochrony danych osobowych oraz zasady ochrony i przetwarzania danych osobowych obowiązujące w Agencji Restrukturyzacji i Modernizacji Rolnictwa. Zobowiązuję się do zachowania w tajemnicy/poufności danych osobowych przetwarzanych w Agencji Restrukturyzacji i Modernizacji Rolnictwa oraz sposobu ich zabezpieczenia w czasie trwania zatrudnienia oraz po zaprzestaniu wykonywania pracy, a także do przetwarzania danych wyłącznie w granicach upoważnienia, w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

…….
*(data i podpis osoby upoważnionej)*

**Pouczenie:**

*- wypełnić wstawiając: imię i nazwisko, indywidualny numer pracownika nadany w systemie kadrowo-płacowym ARiMR (KIP), jednostka organizacyjna, w której wykonywana jest praca.
Dla innej osoby niż pracownik: imię i nazwisko, określenie statusu prawnego (np. wolontariusz, stażysta, praktykant, zleceniobiorca itp.) ze wskazaniem jednostki organizacyjnej ARiMR, w której wykonuje pracę.

** **należy zaznaczyć obydwa checkbox-y jedynie w przypadku, gdy zakres czynności obejmuje przetwarzanie danych osobowych zwykłych i przetwarzanie danych osobowych szczególnych kategorii, o których mowa w art. 9 Rozporządzenia, tj. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków**

**zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej. W pozostałych przypadkach należy zaznaczyć jedynie checkbox dotyczący danych osobowych zwykłych i przekreślić checkbox dotyczący danych szczególnych kategorii.**

*** - wynika z zakresu obowiązków pracowniczych lub innej podstawy wykonywania pracy.

| **Wykaz osób upoważnionych do przetwarzania danych poza zbiorami w Centrali ARiMR/…….. OR ARiMR*** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Lp.** | **Imię i Nazwisko** | **Jednostka organiz.** | **Komórka organiz.**** | **Data nadania upoważnienia** | **Upoważniony (a) w zakresie wykonywania *** ** | | **Data odbioru upoważnienia** | **Uwagi** |
| | | | | | **obowiązków pracowniczych** | **innych obowiązków** | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | |

* Niepotrzebne skreślić
** Wypełniać tylko dla osób nie będących pracownikami
*** Wstawić X w odpowiedniej kolumnie

*Załącznik nr 4 do Regulaminu ochrony danych osobowych*

Znak sprawy:

**UPOWAŻNIENIE**
**DO PRZETWARZANIA DANYCH OSOBOWYCH**
**w zbiorach przetwarzanych w formie papierowej**

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem",

**upoważniam / odbieram upoważnienie*:**

Panią/Pana*……..,

posiadającą/ego nr. KIP – ……..,

zatrudnioną/ego w …….. ARiMR,
*(komórka organizacyjna)*

do przetwarzania danych osobowych w zbiorze:

……

……

w następującym zakresie:

……

……

……

.....
*(data, pieczątka imienna i podpis Właściciela zbioru/dyrektora OR)**

* Niepotrzebne skreślić

| **Wykaz umów powierzenia przetwarzania danych osobowych zawartych w Centrali/..... OR* ARiMR w ..... roku** | | | | | | |
|---|---|---|---|---|---|---|
| **Lp.** | **Data i nr umowy na wykonanie usługi oraz opis przedmiotu umowy **** | **Data i nr Umowy powierzenia przetwarzania** | **Strona Umowy powierzenia przetwarzania** | **Komórka organizacyjna nadzorująca wykonanie Umowy** | **Właściciel zbioru lub zbiór danych podlegający powierzeniu** | **Uwagi** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| | | | | | | |

* Wypełnić właściwe, niepotrzebne skreślić.
****** Dotyczy umowy, do której zawarto umowę powierzenia przetwarzania danych osobowych .

## KLAUZULA INFORMACYJNA W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

W związku z treścią 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 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2)), dalej: „RODO", Zamawiający informuje, 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 70, 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. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. b lub c RODO w celu zawarcia oraz wykonania niniejszej umowy lub wypełnienia obowiązku prawnego ciążącego na Administratorze.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429),
   2) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   3) podmioty przetwarzające dane osobowe w imieniu Administratora na mocy zawartych innych umów, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania Umowy zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia umowy.

## OŚWIADCZENIE O WYPEŁNIENIU OBOWIĄZKU INFORMACYJNEGO

Oświadczenie Wykonawcy wobec Agencji Restrukturyzacji i Modernizacji Rolnictwa o wypełnieniu obowiązku informacyjnego wobec innych osób fizycznych

1) Wykonawca oświadcza, że dane osobowe osób fizycznych, przekazane Agencji Restrukturyzacji i Modernizacji Rolnictwa w ramach realizacji umowy, które zostały pozyskane w sposób bezpośredni lub pośredni przetwarza zgodnie z obowiązującymi w tym zakresie regulacjami prawnymi;
2) Wykonawca oświadcza, że jest uprawniony do przekazania ARiMR danych osobowych, o których mowa w pkt. 1 oraz że uczynił zadość wszelkim obowiązkom związanym z ich przekazaniem, a w szczególności poinformował osoby fizyczne, których dane przekazuję, o fakcie i celu ich przekazania;
3) Wykonawca oświadcza, że wypełnił obowiązek informacyjny wynikający z treści 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 (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016 r., str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., str. 2), zwanego dalej "Rozporządzeniem", wobec wszystkich osób fizycznych, o których mowa w pkt. 1, poprzez przekazanie do ich wiadomości treści Klauzuli informacyjnej dotyczącej przetwarzania przez Agencję Restrukturyzacji i Modernizacji Rolnictwa danych osobowych osób fizycznych, pozyskanych w sposób pośredni od Wykonawcy, stanowiącej Załącznik nr 7A do niniejszej Umowy;
4) Wykonawca oświadcza, że wobec osób fizycznych, których dane osobowe będzie zobowiązany przekazać ARiMR w przyszłości, wypełni obowiązek informacyjny wynikający z treści art. 14 Rozporządzenia, poprzez poinformowanie wszystkich tych osób o treści Klauzuli informacyjnej dotyczącej przetwarzania przez Agencję Restrukturyzacji i Modernizacji Rolnictwa danych osobowych osób fizycznych, pozyskanych w sposób pośredni od Wykonawcy, stanowiącej Załącznik nr 7A do niniejszej Umowy.

(data, podpisy)

1. ……,

2. ……,

* W przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa.

*ZAŁĄCZNIK NR 7A DO UMOWY ...../DI/2020/2610 Z DNIA.....2020 R.*

**Klauzula informacyjna dotycząca przetwarzania przez Agencję Restrukturyzacji i Modernizacji Rolnictwa danych osobowych osób fizycznych**

Zgodnie z treścią z 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 (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), zwanego dalej: „RODO", w odniesieniu do danych osobowych osób fizycznych, które zostały pozyskane przez:

……..

*(nazwa Wykonawcy)*

w ramach (…) Agencja Restrukturyzacji i Modernizacji Rolnictwa informuje, że:

1) Administratorem Pani/Pana danych osobowych (zwanym dalej: "Administratorem danych") w związku z realizacją zadań, o których mowa w pkt. 4 poniżej, jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II 70, 00-175 Warszawa;
2) z Administratorem danych 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;
3) Administrator danych wyznaczył inspektora ochrony danych, z którym może Pani/Pan kontaktować się w sprawach dotyczących przetwarzania Pani/Pana danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych osobowych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora danych, wskazany w pkt 2;
4) Pani/Pana dane osobowe pozyskane przez Administratora danych przetwarzane będą na podstawie art. 6 ust. l lit. b lub c RODO, w celu realizacji umowy lub wypełnienia obowiązku prawnego ciążącego na Administratorze;
5) na podstawie, o której mowa w pkt. 4 Administrator danych będzie przetwarzał następujące kategorie Pani/Pana danych osobowych: dane identyfikacyjne oraz dane kontaktowe;
6) odbiorcami Pani/Pana danych osobowych, przetwarzanych zgodnie z pkt. 4 mogą być:
   a) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   b) podmioty przetwarzające dane osobowe na zlecenie Administratora danych w związku z wykonywaniem powierzonego im zadania w drodze zawartej umowy, m.in. dostawcy wsparcia informatycznego;
7) Pani/Pana dane osobowe, zebrane na podstawie, o której mowa w pkt. 4, będą przetwarzane przez Administratora danych przez okres 4 lat. Okres przetwarzania Pani/Pana danych osobowych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora danych. Ponadto, okres przechowywania danych może zostać przedłużony o okres potrzebny do przeprowadzenia archiwizacji;
8) przysługuje Pani/Panu prawo dostępu do Pani/Pana danych osobowych, prawo żądania ich sprostowania, usunięcia lub ograniczenia przetwarzania.
9) w przypadku uznania, że przetwarzanie Pani/Pana danych osobowych narusza przepisy Rozporządzenia, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
10) Pani/Pana dane Administrator uzyskał od Wykonawcy.

*ZAŁĄCZNIK NR 8 DO UMOWY ...../DI/2020/2610 Z DNIA.....2020 R.*

**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

..... – zwaną dalej **„Wykonawcą",** reprezentowaną przez:

.....

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

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

1. W celu wykonania Umowy nr ...../DI/2020/2610 z dnia ……2020 r. (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 dnia 04.05.2016 r., str. 1, ze zm.), zwanego również „Rozporządzenie" lub „ogólne rozporządzenie o ochronie danych", przetwarzanie danych osobowych znajdujących się w systemie teleinformatycznym ARiMR w zbiorze/zbiorach/zasobach: ....., a Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.
2. 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.
3. Na podstawie Umowy powierzenia przetwarzania danych osobowych Strony określają jej przedmiot w następujący sposób:
   1) Zamawiający powierza Wykonawcy przetwarzanie danych osobowych w zakresie[2]:
      a) charakter przetwarzania:.....;
      b) kategoria osób, których dane dotyczą:.....;
      c) rodzaj danych osobowych:.....;
   2) Zamawiający powierza Wykonawcy przetwarzanie danych osobowych poprzez wykonanie następujących operacji na powierzonych danych osobowych[3]:

[2] Należy dokładnie określić: charakter przetwarzania (tj. zespół cech właściwych całemu procesowi lub poszczególnych operacji przetwarzania, np. przetwarzanie danych może odbywać się elektronicznie lub w formie papierowej, w sposób zautomatyzowany, półautomatycznie lub ręcznie; przetwarzanie danych może odbywać się także w sposób ciągły, systematyczny lub sporadyczny; charakter (operacji) przetwarzania danych to sposób ich dokonywania – częstotliwość/powtarzalność, czasowość, długoterminowość, masowość z uwzględnieniem zastosowanych technologii); kategorię osób, których dane dotyczą (tj. informacje dotyczące charakterystyki określonej grupy podmiotów danych, np. dane pracowników Administratora, dane producenta rolnego/beneficjenta); rodzaj danych osobowych (np. dane zwykłe lub dane szczególnych kategorii, o których mowa w art. 9 ogólnego rozporządzenia o ochronie danych lub dane z art. 10 ogólnego rozporządzenia o ochronie danych, w postaci: np. imienia i nazwiska, adresu zamieszkania, nr PESEL, nr telefonu, nr producenta rolnego, nr działki ewidencyjnej).

[3] Należy dokładnie określić rodzaj wykonywanych operacji na powierzonych danych osobowych, np. utrwalanie (tj. kopiowanie, zapisywanie), przechowywanie (tj. archiwizowanie, wykonywanie kopii bezpieczeństwa, zapisywanie na nośnikach danych i w pamięci komputerów), opracowywanie (tj. analizowanie, porównywanie,

a) ……..;
b) ……..;
c) ……..;
d) ……..

4. Dane osobowe będą przekazane Wykonawcy przez Zamawiającego poprzez nadanie osobom wskazanym przez Wykonawcę praw dostępu do systemu teleinformatycznego ARiMR, w którym te dane się znajdują, dostępnego w[4] …….
5. Wniosek o nadanie uprawnień dostępu do systemu teleinformatycznego ARiMR przez Zamawiającego osobom wskazanym przez Wykonawcę, potwierdzać będzie na piśmie upoważniony pełnomocnik Wykonawcy.
6. 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.
7. Strony ustalają, że odwołanie przez Wykonawcę umocowania udzielonego pełnomocnikowi, o którym mowa w ust. 5 dokonywane będzie na piśmie. O każdorazowym odwołaniu wskazanego powyżej upoważnienia Wykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego w formie pisemnej.
8. 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.
9. Wykonawca zobowiązuje się niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie, o którym mowa w ust. 8 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 jest uprawniony do dalszego przekazywania (tzw. podpowierzania) danych osobowych uzyskanych od Zamawiającego w trybie powierzenia.
4. 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.
5. Wykonawca zobowiązuje się wykonać wszelkie czynności i zobowiązania wynikające z Umowy Powierzenia i ogólnego rozporządzenia o ochronie danych z najwyższą starannością.
6. 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.
7. Wykonawca zobowiązuje się niezwłocznie, ale nie później niż w ciągu 3 (trzech) 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.
8. 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

testowanie), zmienianie (tj. modyfikowanie, dezintegrowanie), usuwanie (tj. kasowanie z nośników danych i pamięci komputerów, niszczenie danych) itp.

[4] Należy dokładnie określić miejsce (tj. adres), w którym będzie umożliwiony dostęp do systemu teleinformatycznego ARiMR (np. siedziba Wykonawcy).

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.

9. 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.

**§ 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,
5) [5].....

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 20.000,00zł (słownie: dwadzieścia tysięcy 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 10.000,00 zł (słownie: dziesięć tysięcy 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 10.000,00 zł (słownie: dziesięć tysięcy złotych) 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.

[4] Wymienić inne uprawnienia upoważnionych pracowników Zamawiającego, związane z wykonaniem audytu, np. uczestniczenie w procesie migracji danych osobowych.

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 § 3 ust. 2 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.

**§ 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 (…), tel. (…), e-mail (…);
   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: (…);
   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

……. ……

*ZAŁĄCZNIK NR 8A DO UMOWY ...../DI/2020/2610 Z DNIA.....2020 R.*

**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 **„Podwykonawcą",** reprezentowanym(ą) przez:

……...

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

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

1. W celu wykonania Umowy nr ……../DI/2020/2610 z dnia ……2020 r. (dalej zwana także – „Umową") zawartej pomiędzy Zamawiającym a[6] …… (Wykonawcą), Zamawiający powierza Podwykonawcy 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 dnia 04.05.2016 r., str. 1, ze zm.), zwanego również „Rozporządzenie" lub „ogólne rozporządzenie o ochronie danych", przetwarzanie danych osobowych znajdujących się w systemie teleinformatycznym ARiMR w zbiorze/zbiorach/zasobach: ……..., a Podwykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych w powyższym celu, w zakresie i w sposób niezbędny do wykonania Umowy.
2. Podwykonawca 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. Podwykonawca 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.
3. Na podstawie Umowy powierzenia przetwarzania danych osobowych Strony określają jej przedmiot w następujący sposób:
   3) Zamawiający powierza Podwykonawcy przetwarzanie danych osobowych w zakresie[7]:

[6] Należy wpisać Wykonawcę, na rzecz którego Podwykonawca wykonuje obowiązki w ramach Umowy głównej.

[7] Należy dokładnie określić: charakter przetwarzania (tj. zespół cech właściwych całemu procesowi lub poszczególnych operacji przetwarzania, np. przetwarzanie danych może odbywać się elektronicznie lub w formie papierowej, w sposób zautomatyzowany, półautomatycznie lub ręcznie; przetwarzanie danych może odbywać się także w sposób ciągły, systematyczny lub sporadyczny; charakter (operacji) przetwarzania danych to sposób ich dokonywania – częstotliwość/powtarzalność, czasowość, długoterminowość, masowość z uwzględnieniem zastosowanych technologii); kategorię osób, których dane dotyczą (tj. informacje dotyczące charakterystyki określonej grupy podmiotów danych, np. dane pracowników Administratora, dane producenta rolnego/beneficjenta); rodzaj danych osobowych (np. dane zwykłe lub dane szczególnych kategorii, o których mowa w art. 9 ogólnego rozporządzenia o ochronie danych lub dane z art. 10 ogólnego rozporządzenia o ochronie

a) charakter przetwarzania:……..;

b) kategoria osób, których dane dotyczą:……..……..;

c) rodzaj danych osobowych:……..……..;

4) Zamawiający powierza Podwykonawcy przetwarzanie danych osobowych poprzez wykonanie następujących operacji na powierzonych danych osobowych[8]:

e) ……..;

f) ……..;

g) ……..;

h) ……..

4. Dane osobowe będą przekazane Podwykonawcy przez Zamawiającego poprzez nadanie osobom wskazanym przez Podwykonawcę praw dostępu do systemu teleinformatycznego ARiMR, w którym te dane się znajdują, dostępnego w[9] ……
5. Wniosek o nadanie uprawnień dostępu do systemu teleinformatycznego ARiMR przez Zamawiającego osobom wskazanym przez Podwykonawcę, potwierdzać będzie na piśmie upoważniony pełnomocnik Wykonawcy i pełnomocnik Podwykonawcy.
6. Dane osobowe zostaną przekazane przez Zamawiającego po dostarczeniu mu przez Podwykonawcę 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 Podwykonawcę, który w terminie 3 dni po każdej zmianie obszarów przetwarzania powierzonych danych jest obowiązany dostarczyć Zamawiającemu nowy wykaz obszarów ich przetwarzania.
7. Strony ustalają, że odwołanie przez Podwykonawcę umocowania udzielonego pełnomocnikowi, o którym mowa w ust. 5 dokonywane będzie na piśmie. O każdorazowym odwołaniu wskazanego powyżej upoważnienia Podwykonawca zobowiązany jest niezwłocznie poinformować Zamawiającego w formie pisemnej.
8. Podwykonawca 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 Podwykonawcę wynika z obowiązujących przepisów prawa unijnego lub krajowego, Podwykonawca 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.
9. Podwykonawca zobowiązuje się niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie, o którym mowa w ust. 8 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 Podwykonawcy 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 Podwykonawca przyjmuje do przetwarzania dane osobowe wyłącznie w celu i zakresie niezbędnym do wykonania Umowy, o której mowa w § 1 ust. 1 Umowy Powierzenia.
3. Podwykonawca nie jest uprawniony do dalszego przekazywania (tzw. podpowierzania) danych osobowych uzyskanych od Zamawiającego w trybie powierzenia.
4. Podwykonawca 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.

danych, w postaci: np. imienia i nazwiska, adresu zamieszkania, nr PESEL, nr telefonu, nr producenta rolnego, nr działki ewidencyjnej.

[8] Należy dokładnie określić rodzaj wykonywanych operacji na powierzonych danych osobowych, np. utrwalanie (tj. kopiowanie, zapisywanie), przechowywanie (tj. archiwizowanie, wykonywanie kopii bezpieczeństwa, zapisywanie na nośnikach danych i w pamięci komputerów), opracowywanie (tj. analizowanie, porównywanie, testowanie), zmienianie (tj. modyfikowanie, dezintegrowanie), usuwanie (tj. kasowanie z nośników danych i pamięci komputerów, niszczenie danych) itp.

[9] Należy dokładnie określić miejsce (tj. adres), w którym będzie umożliwiony dostęp do systemu teleinformatycznego ARiMR (np. siedziba Podwykonawcy).

5. Podwykonawca zobowiązuje się wykonać wszelkie czynności i zobowiązania wynikające z Umowy Powierzenia i ogólnego rozporządzenia o ochronie danych z najwyższą starannością.
6. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Zamawiającego za przetwarzanie powierzonych danych osobowych, Podwykonawca zobowiązuje się niezwłocznie zawiadomić o tych zagrożeniach Zamawiającego i podjąć wszelkie działania niezbędne dla usunięcia tych zagrożeń oraz natychmiast zawiadomić Zamawiającego o podjętych działaniach.
7. Podwykonawca zobowiązuje się niezwłocznie, ale nie później niż w ciągu 3 (trzech) 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 Podwykonawcy, a także o wszelkich zaplanowanych lub prowadzonych kontrolach i inspekcjach u Podwykonawcy, dotyczących przetwarzania powierzonych danych.
8. 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, Podwykonawca 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. Podwykonawca niniejszym zobowiązuje się do zapewnienia Zamawiającemu na swój koszt ochrony sądowej oraz do poniesienia konsekwencji zapadłego wyroku sądowego.
9. Podwykonawca 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.

**§ 3**
**Zabezpieczenie powierzonych danych osobowych.**

1. Podwykonawca 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. Podwykonawca 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 Podwykonawca 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 Podwykonawcę, w tym sprawdzania, czy środki techniczne i organizacyjne zabezpieczające przetwarzanie powierzonych danych, zastosowane przez Podwykonawcę, odpowiadają ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Ponadto Zamawiający ma prawo dokonać weryfikacji, czy Podwykonawca 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 Podwykonawcy udostępnienia dokumentów, złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego,
   4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych Podwykonawca służących do przetwarzania powierzonych danych osobowych,
   5) [10.] .....
3. Z czynności audytowych przeprowadzający audyt pracownicy Zamawiającego sporządzają protokół w dwóch egzemplarzach – podpisany przez przedstawicieli obu Stron - z których jeden egzemplarz doręcza się Podwykonawcy.
4. Podwykonawca 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 Podwykonawcy, 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, Podwykonawca zobowiązuje się do ich usunięcia w wyznaczonym przez Zamawiającego terminie. W razie niezastosowania się przez Podwykonawcę do wydanych mu poleceń, w tym m.in. w przypadku nieusunięcia przez Podwykonawcę wskazanej mu nieprawidłowości w wyznaczonym terminie, Zamawiający może naliczyć Podwykonawcy karę umowną w wysokości 10.000,00 zł (słownie: dziesięć tysięcy złotych) za każdy przypadek stwierdzonej i nieusuniętej w terminie nieprawidłowości.
6. Jeżeli nieprawidłowości wskazane w ust. 5 zostaną ponownie ujawnione, Zamawiający może naliczyć Podwykonawcy karę umowną w wysokości wskazanej w ust. 5 bez wyznaczania terminu do usunięcia tych nieprawidłowości.
7. W przypadku naliczenia kary umownej, Zamawiający wezwie Podwykonawcę 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, Podwykonawca 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 Podwykonawcę 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 Podwykonawcę 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.

[10.] Wymienić inne uprawnienia upoważnionych pracowników Zamawiającego, związane z wykonaniem audytu, np. uczestniczenie w procesie migracji danych osobowych.

5. W przypadku niewykonania przez Podwykonawcę zobowiązania wynikającego z treści §5 ust. 2 Umowy Powierzenia Zamawiający uprawniony jest do naliczenia Podwykonawcy 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 § 4 ust. 7 Umowy Powierzenia.
6. W przypadku naruszenia przez Podwykonawcę zobowiązania, o którym mowa w § 3 ust. 2 pkt 5, Zamawiający uprawniony jest do naliczenia Podwykonawcy kary umownej w wysokości 10.000,00 zł (słownie: dziesięć tysięcy złotych) 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. Z tytułu wykonania Umowy Powierzenia Podwykonawcy nie przysługuje wynagrodzenie.
2. Wykonanie Umowy Powierzenia nie może być podstawą dodatkowych roszczeń Podwykonawcy wobec Zamawiającego.
3. Uprawnienie Zamawiającego względem Podwykonawcy do kary umownej oraz odszkodowań wskazanych w niniejszej Umowie Powierzenia nie wyłącza odpowiedzialności Podwykonawcy w przypadku wystąpienia zdarzenia, o którym mowa w §2 ust. 8 niniejszej Umowy Powierzenia.

**§ 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:
   c) Administratora na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…);
   d) Podwykonawcy na następujące dane kontaktowe: adres (…), tel. (…), e-mail (…).
5. Dane przedstawicieli Stron:
   a) Administratora w kontaktach z Podwykonawcą w zakresie ustaleń Umowy Powierzenia reprezentować będą następujące osoby: (…);
   b) Podwykonawcę 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 Podwykonawcy.

ZAMAWIAJĄCY PODWYKONAWCA

..... .....

ZAŁĄCZNIK NR 9 DO UMOWY …...../DI/2020/2610 Z DNIA……2020 R..

**Formularz ofertowy**

**Załącznik nr 6 do SIWZ**

**Plik, w formacie xml, wygenerowany z narzędzia ESPD**

**Plik, w formacie xml, wygenerowany z narzędzia ESPD („ESPD") znajduje się w odrębnym pliku o nazwie „Załącznik nr 6 do SIWZ ESPD". Plik należy pobrać i zapisać na dysk komputera oraz wypełnić przy pomocy narzędzia udostępnionego przez Urząd Zamówień Publicznych pod adresem https://espd.uzp.gov.pl .**

**Po uruchomieniu wyżej wymienionej strony internetowej, należy wybrać „pl Polski", a potem zaznaczyć „Jestem wykonawcą". Następnie należy zaimportować „ESPD" wczytując plik będący Załącznikiem nr 6 do SIWZ. Po sporządzeniu JEDZ należy go podpisać przez osobę lub osoby uprawnione.**

Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia należy złożyć w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomocą środka komunikacji elektronicznej tj. Platformę Zakupową.

Szczegółowy zakres wymagań określony został w Rozdziale IV.2 SIWZ.