załącznik nr 1 doUchwały nr 10637/2023
Zarządu Województwa Opolskiego
z dnia 9 października 2023 r.

UMOWA delegowania zadań Agencji Płatniczej nr ……..

zawarta pomiędzy

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II nr 70, 00-175 Warszawa, działającą jako „agencja płatnicza", reprezentowaną przez:

1. Panią Halinę Szymańską – Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa;

a

Samorządem Województwa……..……z siedzibą w ……, zwanym dalej „podmiotem wdrażającym", reprezentowanym przez:

1. ……
2. …….....

W związku z realizacją obowiązków wynikających z Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023-2027, zwanego dalej „Planem Strategicznym" oraz:

- na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/2115 z dnia 2 grudnia 2021 r. ustanawiającego przepisy dotyczące wsparcia planów strategicznych sporządzanych przez państwa członkowskie w ramach wspólnej polityki rolnej (planów strategicznych WPR) i finansowanych z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i z Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz uchylającego rozporządzenia (UE) nr 1305/2013 i (UE) nr 1307/2013, zwanego dalej „rozporządzeniem 2021/2115";
- na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/2116 z dnia 2 grudnia 2021 r. w sprawie finansowania wspólnej polityki rolnej, zarządzania nią i monitorowania jej oraz uchylenia rozporządzenia (UE) nr 1306/2013, zwanego dalej „rozporządzeniem 2021/2116";
- uwzględniając kryteria akredytacji określone w pkt 1.D.1 załącznika I do rozporządzenia delegowanego Komisji (UE) 2022/127 z dnia 7 grudnia 2021 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/2116 o przepisy dotyczące agencji płatniczych i innych organów, zarządzania finansami, rozliczania rachunków, zabezpieczeń oraz stosowania euro, zwanego dalej „rozporządzeniem 2022/127";
- uwzględniając ustawę z dnia 8 lutego 2023 r. o Planie Strategicznym dla Wspólnej Polityki Rolnej na lata 2023–2027, zwaną dalej „ustawą PS WPR";
- uwzględniając ustawę z dnia 9 maja 2008 r. o Agencji Restrukturyzacji i Modernizacji Rolnictwa, zwaną dalej „ustawą o ARiMR";
- uwzględniając ustawę z dnia 26 stycznia 2023 r. o finansowaniu wspólnej polityki rolnej na lata 2023–2027, zwaną dalej „ustawą o finansowaniu WPR",

Strony ustalają następujące zasady współpracy i podział obowiązków przy realizacji niniejszej umowy.

§ 1.

Określenia i skróty

Użyte w umowie określenia i skróty oznaczają:

1) **Agencja płatnicza** – agencję płatniczą w rozumieniu art. 9 ust. 1 rozporządzenia 2021/2116;
2) **beneficjent** – beneficjenta w rozumieniu art. 3 pkt 13 rozporządzenia 2021/2115;
3) **EFRROW** – Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich;
4) **ETO** – Europejski Trybunał Obrachunkowy;
5) **Instytucja Zarządzająca** – instytucję zarządzającą w rozumieniu art. 123 rozporządzenia 2021/2115;
6) **interwencja** – interwencję w rozumieniu art. 3 pkt 3 rozporządzenia 2021/2115;
7) **KAS** – Krajową Administrację Skarbową;
8) **KE** – Komisję Europejską;
9) **kontrola administracyjna –** kontrolę administracyjną, o której mowa w pkt 1.A ppkt (i) załącznika I do rozporządzenia 2022/127 oraz w rozdziale 6 ustawy PS WPR;
10) **kontrola na miejscu** – kontrolę na miejscu, o której mowa w pkt 1.A ppkt (i) załącznika I do rozporządzenia 2022/127 oraz w rozdziale 6 ustawy PS WPR;
11) **LGD –** lokalną grupę działania realizującą LSR, z którą zarząd województwa zawarł umowę ramową w ramach konkursu na perspektywę programowania 2023-2027;
12) **LSR –** strategię rozwoju lokalnego kierowanego przez społeczność, o której mowa w ustawie z dnia 20 lutego 2015 r. o rozwoju lokalnym z udziałem lokalnej społeczności;
13) **moduł LGD** – część systemu IT dedykowana LGD do wykonywania określonych zadań;
14) **monitoring prawidłowości wykonywania zadań delegowanych** – monitorowanie prawidłowości wykonywania zadań delegowanych w zakresie i na zasadach określonych w § 18 ust. 1-3;
15) **NIK** – Najwyższą Izbę Kontroli;
16) **operacja** – operację w rozumieniu art. 3 pkt 4 rozporządzenia 2021/2115;
17) **podmiot wdrażający** – Samorząd Województwa, który wykonuje zadania agencji płatniczej jako zadania delegowane, zgodnie z art. 10 ust. 3 ustawy PS WPR;
18) **podstawa systemu realizacji Planu Strategicznego** – postanowienia Planu Strategicznego, przepisy prawa powszechnie obowiązującego, wytyczne instytucji zarządzającej oraz regulaminy naborów wniosków o przyznanie pomocy;
19) **rozporządzenie 2016/679** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 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);
20) **stanowisko wrażliwe** – stanowisko pracy, na którym pracownik w związku z wykonywanymi czynnościami służbowymi, może być narażony na ryzyko wystąpienia zdarzeń korupcyjnych lub konfliktu interesów;
21) **system IT –** system teleinformatyczny ARiMR, o którym mowa w art. 10c ustawy o ARiMR;

22) **umowa o przyznaniu pomocy** – umowę o przyznaniu pomocy, o której mowa w art. 94 ust. 1 ustawy PS WPR, zawieraną z beneficjentem;

23) **umowa ramowa** – umowę o warunkach i sposobie realizacji LSR zawieraną między Zarządem Województwa i LGD, której LSR została wybrana do finansowania w okresie programowania 2023–2027;

24) **ustawa o ochronie danych osobowych –** ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;

25) **wytyczne** – wytyczne instytucji zarządzającej, o których mowa w art. 6 ust. 2 pkt 3 ustawy PS WPR.

§ 2.

Przedmiot umowy

1. Umowa określa szczegółowy zakres zadań delegowanych przez agencję płatniczą, zwanych dalej „zadaniami delegowanymi", do podmiotu wdrażającego, warunki i sposób ich realizacji, zakres odpowiedzialności i obowiązki stron oraz rodzaj informacji i dokumentów towarzyszących, które są przekazywane agencji płatniczej oraz terminy ich przekazywania.
2. Zadania delegowane, o których mowa w art. 10 ust. 3 i 4 ustawy PS WPR oraz w umowie, dotyczące interwencji:
   - Scalanie gruntów wraz z zagospodarowaniem poscaleniowym (I.10.8.),
   - Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi (I.10.10.),
   - LEADER/Rozwój Lokalny Kierowany przez Społeczność (I.13.1),

   obejmują w szczególności:
   1) prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy, w tym:
      a) przeprowadzanie kontroli administracyjnych,
      b) dokonywanie wyboru operacji,
      c) zawieranie i zmianę umów, na podstawie których jest przyznawana pomoc, informowanie o odmowie jej przyznania i odmowie zawarcia umowy oraz rejestrowanie tych umów i informacji;
   2) przeprowadzanie kontroli na miejscu;
   3) ustalanie kwot z tytułu nienależnie lub nadmiernie pobranych płatności i wzywanie beneficjenta do zwrotu tych kwot;
   4) przechowywanie dokumentów związanych z wykonywaniem przez podmiot wdrażający zadań agencji płatniczej;
   5) udostępnianie lub przekazywanie agencji płatniczej, instytucji zarządzającej, Komisji Europejskiej lub innym organom upoważnionym do kontroli, dokumentów, o których mowa w pkt 4;
   6) zatwierdzanie płatności na rzecz beneficjenta;
   7) rozpatrywanie środków zaskarżenia na etapie przyznania/wypłaty pomocy finansowej;

8) prognozowanie wydatków oraz przekazywanie do agencji płatniczej w formie elektronicznej prognoz wydatków, o których mowa w § 11.

3. Zadania delegowane są wykonywane pod warunkiem posiadania przez agencję płatniczą akredytacji, o której mowa w art. 2 ust. 1 pkt 1 ustawy o finansowaniu WPR.

4. Realizacja zadań delegowanych będzie finansowana ze środków pomocy technicznej, o której mowa w art. 125 rozporządzenia 2021/2115 do wysokości limitu środków dostępnych dla Samorządu Województwa …….(nazwa województwa), określonego przez Ministra Rolnictwa i Rozwoju Wsi, zgodnie z art. 111 ust. 1 ustawy PS WPR. Kwestię uruchamiania środków na wyprzedzające finansowanie kosztów kwalifikowalnych w ramach pomocy technicznej dla Samorządu Województwa określa ustawa o finansowaniu WPR.

§ 3.

Prawa i obowiązki stron

1. Do obowiązków agencji płatniczej należy:

1) opracowanie i aktualizacja jednolitych procedur, instrukcji postępowania związanych z realizacją zadań delegowanych, przy udziale podmiotu wdrażającego, zgodnie z *Zasadami przepływu informacji dotyczącymi szczegółowych warunków i trybu przyznawania i zatwierdzania pomocy finansowej oraz stosowania procedur w zakresie zadań delegowanych przez agencję płatniczą do podmiotów wdrażających w ramach Planu Strategicznego*, zwanymi dalej „Zasadami przepływu informacji", przekazanymi przez agencję płatniczą w terminie miesiąca przed przyjęciem tych zasad do stosowania przez podmiot wdrażający;

2) przekazywanie podmiotowi wdrażającemu procedur i instrukcji, o których mowa w pkt 1, z podaniem terminu ich przyjęcia do wewnętrznego stosowania, który nie powinien być krótszy niż miesiąc od dnia przekazania tych procedur i instrukcji; przy czym istnieje możliwość skrócenia ww. terminu, w uzgodnieniu z podmiotem wdrażającym, zgodnie z Zasadami przepływu informacji;

3) opracowanie i przekazanie podmiotowi wdrażającemu wzorów regulaminów naborów wniosków o przyznanie pomocy ogłaszanych przez SW;

4) zapewnienie podmiotowi wdrażającemu, a także LGD, systemu IT, o którym mowa w § 4, oraz jego aktualizacji, obejmujących w szczególności system elektroniczny do rejestrowania i przechowywania najważniejszych informacji na temat wdrażania Planu Strategicznego, które są potrzebne do monitorowania i ewaluacji postępów w osiąganiu ustalonych celów, o których mowa w art. 130 rozporządzenia 2021/2115;

5) przeprowadzanie szkoleń w zakresie stosowania procedur, o których mowa w pkt 1, oraz obsługi systemu IT, o którym mowa w § 4;

6) udzielanie podmiotowi wdrażającemu wyjaśnień lub dokonywanie interpretacji w zakresie wykonywania zadań delegowanych, w szczególności stosowania procedur i instrukcji, o których mowa w pkt 1, oraz obsługi systemu IT, o którym mowa w § 4, zgodnie z Zasadami przepływu informacji;

7) weryfikacja – w uzasadnionych przypadkach – gotowości podmiotu wdrażającego do wykonywania zadań delegowanych poprzez przeprowadzenie audytu;

8) monitoring prawidłowości wykonywania przez podmiot wdrażający zadań delegowanych, zgodnie z podstawą systemu realizacji Planu Strategicznego, w szczególności z określonymi w

niej trybem i terminami oraz procedurami i instrukcjami, o których mowa w pkt 1, w szczególności poprzez przeprowadzanie regularnych przeglądów delegowanych zadań, o których mowa w pkt 1.D.1 ppkt (vi) załącznika I do rozporządzenia 2022/127 oraz przeprowadzanie kontroli, o których mowa w art. 10 ust. 5 pkt 2 lit. a ustawy PS WPR, do których stosuje się odpowiednio przepisy o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli;

9) przedstawianie podmiotowi wdrażającemu wyników monitoringu, o którym mowa w pkt 8, w formie sprawozdania oraz przekazywanie zaleceń / wniosków / rekomendacji w celu podjęcia przez podmiot wdrażający, w terminach określonych przez agencję płatniczą, odpowiednich czynności zmierzających do usunięcia nieprawidłowości lub poprawy systemu zarządzania i kontroli;

10) przeprowadzanie audytów systemu zarządzania i kontroli, zgodnie z obowiązującymi przepisami prawa i standardami audytu wewnętrznego, w zakresie objętym niniejszą umową, w szczególności przygotowywanie i przekazywanie podmiotowi wdrażającemu zaleceń w zakresie realizacji zadań delegowanych;

11) przekazywanie podmiotowi wdrażającemu wzoru deklaracji zarządczej za dany rok budżetowy oraz wzorów innych dokumentów, zapewniających prawidłową realizację zadań delegowanych;

12) przekazanie podmiotowi wdrażającemu zaleceń w zakresie przygotowania dokumentacji i zapewnienia bezpieczeństwa systemów informacyjnych zgodnie z normą ISO Międzynarodowej Organizacji Normalizacyjnej 27001 – zgodnie z przepisami rozporządzenia 2022/127;

13) przekazanie podmiotowi wdrażającemu zaleceń w zakresie wartości etycznych, przeciwdziałania występowaniu konfliktu interesów, wdrożenia mechanizmów zapewniających nadzór nad stanowiskami wrażliwymi oraz przeciwdziałanie zagrożeniom korupcyjnym lub konfliktowi interesów w obszarze zadań delegowanych;

14) księgowanie zatwierdzonych do wypłaty przez podmiot wdrażający dokumentów i dokonywanie płatności na rzecz beneficjentów;

15) dochodzenie kwot ustalonych przez podmiot wdrażający do zwrotu z tytułu nienależnie lub nadmiernie pobranych środków publicznych;

16) udostępnianie podmiotowi wdrażającemu danych w zakresie niezbędnym dla realizacji zadań delegowanych, zgodnie z postanowieniami Planu Strategicznego, przepisami prawa powszechnie obowiązującego, regulaminami naborów wniosków o przyznanie pomocy oraz procedurami i instrukcjami, o których mowa w pkt 1, zaleceniami / wnioskami / rekomendacjami agencji płatniczej lub wytycznymi Instytucji Zarządzającej, wydawanymi na podstawie art. 6 ust. 2 pkt 3 ustawy PS WPR;

17) przekazywanie podmiotowi wdrażającemu danych w zakresie:

    a) podmiotów wykluczonych z pomocy finansowej zgodnie z przepisami ustawy PS WPR,

    b) podmiotów, które podlegają zakazowi dostępu do środków, o których mowa w art. 5 ust. 3 pkt 4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, na podstawie prawomocnego orzeczenia sądu,

    c) podmiotów, którym nie przysługuje prawo do otrzymania wyprzedzającego finansowania kosztów kwalifikowalnych operacji realizowanych z udziałem środków EFRROW, na podstawie przepisów ustawy o finansowaniu WPR, w związku z wykorzystaniem pożyczki, o której mowa w art. 13 ust. 2 tej ustawy, niezgodnie z przeznaczeniem, pobraniem pożyczki nienależnie lub w nadmiernej wysokości;

18) rejestrowanie informacji o miejscu / miejscach przechowywania dokumentów związanych z wykonywaniem przez podmiot wdrażający zadań delegowanych.

2. Do obowiązków podmiotu wdrażającego należy:

   1) opracowywanie regulaminów naborów wniosków o przyznanie pomocy ogłaszanych przez podmiot wdrażający, z wykorzystaniem wzorów przekazanych przez agencję płatniczą zgodnie z ust. 1 pkt 3, oraz uzgadnianie regulaminów naborów wniosków o przyznanie pomocy ogłaszanych przez LGD;

   2) prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy w systemie IT w sposób określony w podstawie systemu realizacji Planu Strategicznego, a także umowach o przyznaniu pomocy;

   3) przyjęcie do wewnętrznego stosowania procedur i instrukcji, o których mowa w ust. 1 pkt 1, w terminie określonym przez agencję płatniczą, o którym mowa w ust. 1 pkt 2, w tym niepublikowania przyjętych procedur i instrukcji na stronach internetowych urzędu;

   4) realizacja zadań delegowanych zgodnie z trybem i terminami wynikającymi z podstawy systemu realizacji Planu Strategicznego, postanowień umowy oraz procedur i instrukcji, o których mowa w ust. 1 pkt 1;

   5) pozyskiwanie, gromadzenie, opracowywanie i przekazywanie agencji płatniczej danych niezbędnych do właściwego monitorowania realizacji i ewaluacji Planu Strategicznego, zgodnie z art. 11 ustawy PS WPR, w oparciu o system IT, o którym mowa w § 4;

   6) zatwierdzanie płatności na rzecz beneficjentów, w szczególności poprzez sporządzanie i zatwierdzanie zleceń płatności do wypłaty oraz przygotowywanie i przekazywanie agencji płatniczej dokumentów określonych w procedurach i instrukcjach, o których mowa w ust. 1 pkt 1 z informacjami niezbędnymi do dokonywania wypłat środków dla beneficjentów;

   7) ustalanie nienależnie lub nadmiernie pobranych środków publicznych i sporządzanie dokumentów zgłoszenia należności celem rejestracji w Księdze Dłużników oraz zabezpieczenie roszczeń wynikających z niewykonania lub nienależytego wykonania umowy o przyznaniu pomocy przez beneficjenta;

   8) sprawdzanie pod względem zgodności z ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych przeprowadzenia przez beneficjentów postępowań o udzielenie zamówień publicznych w ramach realizacji operacji zgodnie z procedurami i instrukcjami, o których mowa w ust. 1 pkt 1;

   9) przygotowywanie i realizacja kontroli na miejscu, zgodnie z podstawą systemu realizacji Planu Strategicznego oraz procedurami i instrukcjami, o których mowa w ust. 1 pkt 1;

   10) przeciwdziałanie, wykrywanie i przekazywanie agencji płatniczej informacji o nieprawidłowościach i nadużyciach finansowych, zgodnie z procedurami i instrukcjami, o których mowa w ust. 1 pkt 1, w szczególności o prowadzonych postępowaniach karnych wobec beneficjentów, z którymi podmiot wdrażający zawarł umowę o przyznaniu pomocy;

   11) przekazywanie agencji płatniczej informacji o wniesionych i rozpatrywanych skargach i wnioskach dotyczących zadań delegowanych;

   12) rozpatrywanie w zakresie określonym w przepisach ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego odwołań beneficjentów od decyzji administracyjnych w przedmiocie ustalenia kwoty nienależnie lub nadmiernie pobranych środków publicznych;

   13) prowadzenie spraw związanych ze składanymi przez podmioty ubiegające się o przyznanie pomocy / beneficjentów skargami do sądów administracyjnych i pozwami składanymi do sądów powszechnych w przypadkach odmowy przyznania / wypłaty pomocy;

14) umożliwienie przeprowadzenia audytów i kontroli w zakresie zadań delegowanych przez organy KAS, NIK, przedstawicieli KE, ETO, Instytucję Zarządzającą, agencję płatniczą oraz inne uprawnione podmioty oraz przekazywanie agencji płatniczej informacji o powyższych kontrolach, ich wynikach oraz sposobie realizacji zaleceń i wniosków pokontrolnych;

15) umożliwienie agencji płatniczej przeprowadzenia działań monitoringowych, o których mowa w ust. 1 pkt 8 w szczególności kontroli, o której mowa w art. 10 ust. 5 pkt 2 lit. a ustawy PS WPR;

16) umożliwienie agencji płatniczej przeprowadzenia audytu, o którym mowa w art. 10 ust. 5 pkt 2 lit. b ustawy PS WPR;

17) wyznaczenie pracowników, zwanych dalej „trenerami" do udziału w szkoleniach, konsultacjach oraz egzaminach z zakresu stosowania procedur i instrukcji, o których mowa w ust. 1 pkt 1 – w przypadku procedur, co do których nie ma możliwości przeprowadzenia szkoleń w systemie e-szkoleń, o którym mowa w pkt 20, oraz z zakresu obsługi systemu IT, o którym mowa w § 4, oraz modułu LGD;

18) prowadzenie przez trenerów szkoleń, konsultacji zapewniających prawidłowe wykonywanie przez podmiot wdrażający zadań delegowanych;

19) prowadzenie przez podmiot wdrażający szkoleń dotyczących bezpieczeństwa informacji w zakresie wdrożenia zabezpieczeń wynikających z zaleceń, o których mowa w ust. 1 pkt 12;

20) zapewnienie udziału pracowników podmiotu wdrażającego zajmujących się realizacją zadań delegowanych w szkoleniach przeprowadzanych w systemie e-szkoleń udostępnionym przez agencję płatniczą;

21) wdrożenie zaleceń / wniosków / rekomendacji w zakresie prawidłowości realizacji zadań delegowanych, wydanych w wyniku działań monitoringowych, o których mowa w ust. 1 pkt 8 oraz audytów systemu zarządzania i kontroli, o których mowa w art. 10 ust. 5 pkt 2 lit. b ustawy PS WPR;

22) wdrożenie zaleceń / wniosków / rekomendacji w zakresie prawidłowości realizacji zadań delegowanych wskazanych w sprawozdaniach z audytów/kontroli krajowych i unijnych organów kontroli innych niż agencja płatnicza, poprzedzone konsultacjami z agencją płatniczą;

23) wdrożenie i stosowanie, w obszarze dotyczącym zadań delegowanych, o których mowa w § 2 ust. 2, zabezpieczeń wynikających z norm ISO – Międzynarodowej Organizacji Normalizacyjnej 27001 – zgodnie z przepisami rozporządzenia 2022/127 oraz przekazanymi przez agencję płatniczą zaleceniami;

24) zapewnienie w zakresie objętym umową przejrzystego podziału zadań i kompetencji na wszystkich poziomach struktury organizacyjnej podmiotu wdrażającego, zgodnie z zaleceniami wydanymi przez agencję płatniczą poprzez:

    a) określenie na piśmie obowiązków każdego pracownika, któremu powierzono wykonywanie określonych czynności w ramach tych zadań,

    b) powierzenie wykonywania zadań pracownikom posiadającym kwalifikacje lub doświadczenie, oraz odpowiednie przeszkolenie z procedur i instrukcji, o których mowa w ust. 1 pkt 1 oraz z obsługi systemu IT, które zapewniają ich prawidłowe, rzetelne, bezstronne, sprawne i terminowe wykonanie,

    c) stosowanie wartości etycznych oraz niedopuszczenie do wystąpienia konfliktu interesów pomiędzy pracownikami podmiotu wdrażającego, beneficjentami oraz zewnętrznymi usługodawcami;

25) przekazywanie agencji płatniczej informacji dotyczącej podmiotów wykluczonych z pomocy finansowej zgodnie z przepisami ustawy PS WPR oraz zgodnie z procedurami i instrukcjami, o których mowa w ust. 1 pkt 1;

26) wdrożenie mechanizmów zapewniających nadzór nad stanowiskami wrażliwymi oraz przeciwdziałanie zagrożeniom korupcyjnym lub konfliktowi interesów w obszarze zadań delegowanych;

27) sporządzanie i przekazywanie agencji płatniczej prognoz wydatków zgodnie z § 11;

28) przekazywanie agencji płatniczej informacji i dokumentów, określonych w procedurach i instrukcjach, o których mowa w ust. 1 pkt 1 niezbędnych do wszczęcia i prowadzenia postępowania, o którym mowa w ust. 1 pkt 15, w tym zabezpieczenia procesu przechowywania i transportowania prawnych zabezpieczeń/weksli, zgodnie z obowiązującymi normami;

29) ustalanie przez podmiot wdrażający w drodze decyzji administracyjnej kwot nienależnie lub nadmiernie pobranych środków publicznych, również na podstawie zaleceń / wniosków / rekomendacji agencji płatniczej oraz uprawnionych organów, w związku z kontrolą prawidłowości realizacji przez podmiot wdrażający zadań delegowanych oraz wzywanie beneficjenta do zwrotu tych kwot;

30) przekazywanie agencji płatniczej rocznej deklaracji zarządczej w zakresie wykonywania zadań delegowanych wraz z dokumentami potwierdzającymi prawidłową ich realizację;

31) składanie na wezwanie agencji płatniczej wyjaśnień, w szczególności w ramach certyfikacji wydatków lub innych kontroli i audytów przeprowadzanych przez uprawnione organy w związku z realizacją przez podmiot wdrażający zadań delegowanych;

32) zgłaszanie agencji płatniczej, zgodnie z Zasadami przepływu informacji, propozycji, w przypadku stwierdzenia przez podmiot wdrażający konieczności poprawy funkcjonowania systemu zarządzania i kontroli;

33) przekazywanie na wezwanie agencji płatniczej innych informacji, istotnych dla prawidłowej realizacji zadań delegowanych, które nie zostały wymienione w umowie;

34) gromadzenie i przechowywanie dokumentacji związanej z realizacją zadań delegowanych do dnia upływu okresu 5 lat od dnia dokonania przez agencję płatniczą ostatniej płatności w ramach Planu Strategicznego, a jeżeli po upływie tego terminu prowadzone są przez agencję płatniczą postępowania, o których mowa w ust. 1 pkt 15 – do dnia otrzymania przez podmiot wdrażający ostatniej informacji o zakończeniu tych postępowań, o której mowa w § 15 ust. 10 oraz przekazywanie agencji płatniczej informacji o miejscu / miejscach przechowywania dokumentów związanych z wykonywaniem przez podmiot wdrażający zadań delegowanych, zgodnie z procedurami i instrukcjami, o których mowa w ust. 1 pkt 1;

35) udostępnianie lub przekazywanie agencji płatniczej, Instytucji Zarządzającej, KE, ETO lub innym organom upoważnionym do kontroli, zgodnie z odrębnymi przepisami, dokumentacji określonej w pkt 34;

36) informowanie i rozpowszechnianie informacji o interwencjach, o których mowa w § 2 ust. 2, w szczególności podawanie tych informacji do publicznej wiadomości na stronie internetowej urzędu marszałkowskiego, oraz informowanie beneficjentów o obowiązkach wynikających z przyznania pomocy;

37) wykorzystywanie w toku prowadzenia postępowań w sprawach o przyznanie lub wypłatę pomocy systemu Arachne, w przypadku jego wdrożenia w ramach Planu Strategicznego;

38) zapewnienie nadzoru nad LGD, z którymi zarząd województwa zawarł umowę ramową, w zakresie prawidłowego wykorzystywania przez LGD systemu IT - „moduł LGD” - do

obsługi wniosków, w sposób określony w § 4 ust. 3 oraz w dokumencie towarzyszącym do umowy delegowania.

Podmiot wdrażający realizuje w/w zadania w sposób zapewniający prawidłowe, rzetelne, bezstronne, terminowe i bezpieczne wykonanie tych zadań.

3. Ponadto:
   1) Podmiot wdrażający:
      a) ma prawo do przekazywania uwag lub opinii wynikających ze stosowania procedur i instrukcji, o których mowa w ust. 1 pkt 1 lub funkcjonowania systemu zarządzania i kontroli, zgodnie z Zasadami przepływu informacji,
      b) w sprawach delegowanych temu podmiotowi zadań agencji płatniczej związanych z przyznawaniem, wypłatą i zwrotem pomocy może powoływać organy opiniodawczo-doradcze, w skład których mogą wchodzić również osoby niebędące pracownikami tego podmiotu, których udział w pracach takich organów jest uzasadniony zakresem ich zadań;
   2) Agencja płatnicza:
      a) po przekazaniu przez podmiot wdrażający uwag lub opinii wynikających ze stosowania procedur i instrukcji, o których mowa w ust. 1 pkt 1 – dokonuje analizy możliwości ich wdrożenia i każdorazowo przekazuje zwrotną informację, a w przypadku nie uwzględnienia uwag – uzasadnienie ich nieprzyjęcia, zgodnie z Zasadami przepływu informacji,
      b) w sprawach należących do jej zadań związanych z przyznawaniem, wypłatą i zwrotem pomocy może powoływać organy opiniodawczo-doradcze, w skład których mogą wchodzić również osoby niebędące pracownikami tego podmiotu, których udział w pracach takich organów jest uzasadniony zakresem ich zadań;
   3) strony zobowiązują się do:
      a) wymiany informacji i materiałów niezbędnych dla spełnienia wymagań przepisów unijnych i krajowych w zakresie dotyczącym prawidłowej realizacji zadań delegowanych,
      b) przekazywania danych w obustronnie uzgodnionym standardzie, w ramach obowiązujących przepisów prawa, procedur i instrukcji, o których mowa w ust. 1 pkt 1,
      c) sporządzania dokumentacji związanej z realizacją zadań delegowanych, określonej w procedurach i instrukcjach, o których mowa w ust. 1 pkt 1,
      d) zapewnienia w zakresie realizacji umowy, że wykorzystanie danych w zarządzaniu i wdrażaniu Planu Strategicznego odbywać się będzie zgodnie z obowiązującymi przepisami prawa oraz przy zapewnieniu bezpieczeństwa danych,
      e) stosowania Zasad przepływu informacji,
      f) informowania i rozpowszechniania informacji o Planie Strategicznym, w tym określonych w art. 123 ust. 2 lit. k rozporządzenia 2021/2115,
      g) współpracy przy realizacji zadań związanych z realizacją Planu Strategicznego.

§ 4.

Wsparcie realizacji zadań delegowanych systemem IT

1. Agencja płatnicza przed rozpoczęciem realizacji zadań delegowanych udostępnia nieodpłatnie system IT wspierający realizację zadań delegowanych, w szczególności obejmujący elektroniczny system informacyjny, o którym mowa w art. 130 rozporządzenia 2021/2115, służący do obsługi cyfrowych procesów dla interwencji Planu Strategicznego.
2. Podmiot wdrażający w zakresie korzystania z udostępnionego systemu IT zobowiązuje się do:
   1) bieżącego prowadzenia postępowań w sprawie o przyznanie lub wypłatę pomocy;
   2) zapewnienia obsługi wniosków w systemie IT zgodnie z udostępnionymi przez agencję płatniczą instrukcjami;
   3) wykonywania czynności w systemie IT, umożliwiających właściwą realizację zadań delegowanych, w tym sporządzania sprawozdań z wykonywania zadań delegowanych i raportów finansowych;
   4) generowania dokumentów, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1, za pośrednictwem systemu IT;
   5) wprowadzania i aktualizacji danych z umów ramowych zawartych między podmiotem wdrażającym a LGD oraz LSR, w szczególności zapewnienia, że dane będą rzeczywiste, poprawne, prawidłowo zaklasyfikowane, aktualne i kompletne.
3. Podmiot wdrażający, w zakresie korzystania przez LGD z udostępnionego przez agencję płatniczą systemu IT zobowiązuje się do:
   1) przeprowadzania szkoleń dla pracowników LGD, z zakresu obsługi systemu IT w zakresie „modułu LGD”;
   2) zapewnienia nadzoru nad LGD, z którymi zarząd województwa zawarł umowę ramową, w zakresie:
      a) prawidłowego wykonywania zadań w „module LGD” systemu IT, zgodnie z udostępnionymi przez agencję płatniczą instrukcjami,
      b) obsługi wniosków w systemie IT zgodnie z udostępnionymi przez agencje płatniczą instrukcjami,
      c) zgodności między danymi wprowadzonymi do systemu IT, a dokumentami źródłowymi, w szczególności zapewnienia, że dane będą rzeczywiste, poprawne, prawidłowo zaklasyfikowane, aktualne i kompletne.
4. Agencja płatnicza i podmiot wdrażający zobowiązują się wzajemnie w zakresie swoich zadań do wykorzystania systemu IT, o którym mowa w ust. 1, w zarządzaniu i wdrażaniu Planu Strategicznego zgodnie z podstawą systemu realizacji Planu Strategicznego oraz przy zapewnieniu bezpieczeństwa danych, w szczególności wykluczenia dostępu osób nieupoważnionych do danych.
5. Agencja płatnicza i podmiot wdrażający zobowiązują się do nadawania uprawnień do systemu IT, zgodnie z udostępnionymi przez agencję płatniczą instrukcjami, w szczególności:
   1) agencja płatnicza zobowiązuje się do nadawania uprawnień administratora pracownikom podmiotu wdrażającego;
   2) podmiot wdrażający zobowiązuje się do nadawania uprawnień pracownikom podmiotu wdrażającego oraz LGD;

3) podmiot wdrażający zobowiązuje się do przeprowadzania przeglądów uprawnień do systemu IT nadanych pracownikom podmiotu wdrażającego oraz LGD.

§ 5.

Przetwarzanie danych osobowych

1. W przypadku zadań realizowanych przez podmiot wdrażający jako zadania delegowane, agencja płatnicza oraz podmiot wdrażający zobowiązane są do wzajemnego przekazywania danych osobowych, pozyskiwanych w celu realizacji zadań określonych w art. 10 ust. 3 i 4 ustawy PS WPR, po spełnieniu przesłanek legalności przetwarzania, o których mowa w art. 6 rozporządzenia 2016/679.
2. Administratorem danych przetwarzanych w trakcie obsługi wniosku o przyznanie pomocy i wniosku o płatność w rozumieniu rozporządzenia 2016/679, jest podmiot wdrażający.
3. Podmiot wdrażający i agencja płatnicza zobowiązane są do przestrzegania przepisów rozporządzenia 2016/679 i aktualnie obowiązujących przepisów krajowych dotyczących ochrony danych osobowych. Każda ze stron ponosi samodzielną odpowiedzialność za podjęte w tym względzie działania lub za ich zaniechanie.
4. Obowiązek informacyjny agencji płatniczej jako administratora danych osobowych, wynikający z art. 13 i 14 rozporządzenia 2016/679, spełniany jest przez agencję płatniczą w ramach realizacji zadań delegowanych wykonywanych przez podmiot wdrażający, o których mowa w art. 10 ust. 3 i 4 ustawy PS WPR oraz umowie, przy czym treść, formę i sposób realizacji obowiązku informacyjnego ustala agencja płatnicza.
5. Podmiot wdrażający przekaże dokumenty potwierdzające wykonanie obowiązków, o których mowa w ust. 4, na każde żądanie agencji płatniczej w formie i terminie określonym w tym żądaniu.

§ 6.

Gotowość do realizacji zadań i zapewnienia ciągłości realizacji zadań delegowanych

1. Gotowość podmiotu wdrażającego do realizacji zadań delegowanych, poświadczająca spełnienie kryteriów akredytacji, o których mowa w Załączniku I do rozporządzenia 2022/127 właściwych dla Samorządu Województwa oraz warunków określonych w dokumencie towarzyszącym nr 1 do umowy, potwierdzana będzie podpisaniem przez Marszałka Województwa stosownej deklaracji gotowości, według wzoru określonego i przekazanego podmiotowi wdrażającemu przez agencję płatniczą. Po otrzymaniu deklaracji, agencja płatnicza może dokonać oceny gotowości podmiotu wdrażającego, przeprowadzając w jego siedzibie odpowiednie działania audytowe.
2. W przypadku niespełniania, któregokolwiek z warunków określonych w dokumencie towarzyszącym nr 1 do umowy, dopuszczalne jest złożenie warunkowej deklaracji gotowości wraz z „Harmonogramem dojścia do osiągnięcia gotowości do wykonywania przez podmiot wdrażający zadań delegowanych przez agencję płatniczą w ramach PS WPR”, według wzoru określonego i przekazanego podmiotowi wdrażającemu przez agencję płatniczą. W przypadku składania warunkowej deklaracji gotowości dla kilku interwencji, „Harmonogram dojścia …” jest sporządzany odrębnie dla każdej z nich.

3. W przypadku stwierdzenia przez agencję płatniczą, że stan przygotowań podmiotu wdrażającego do realizacji zadań delegowanych nie jest zgodny z podstawą systemu realizacji Planu Strategicznego oraz postanowieniami umowy, agencja płatnicza wydaje zalecenia wraz z terminem na wprowadzenie tych zaleceń.
4. Agencja płatnicza może przeprowadzić audyt wdrożenia zaleceń i potwierdza ostatecznie gotowość podmiotu wdrażającego do realizacji zadań delegowanych. W przypadku niewdrożenia przez podmiot wdrażający zaleceń agencja płatnicza powiadamia o tym fakcie Instytucję Zarządzającą i Ministra Finansów, nie potwierdzając gotowości podmiotu wdrażającego do realizacji zadań.

§ 7.

Prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy

1. Podmiot wdrażający zobowiązuje się do prowadzenia postępowań w sprawach o przyznanie lub wypłatę pomocy w udostępnionym nieodpłatnie systemie IT, o którym mowa w § 4 ust. 1, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1 oraz podstawą systemu realizacji Planu Strategicznego.
2. Podmiot wdrażający przeprowadza kontrolę administracyjną wniosków o przyznanie pomocy oraz wniosków o płatność zgodnie z art. 100 ust. 1–3 ustawy PS WPR.
3. W ramach kontroli administracyjnych podmiot wdrażający zapobiega nieprawidłowemu podwójnemu finansowaniu z innych systemów unijnych lub krajowych i w ramach poprzednich okresów programowania, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.
4. Podmiot wdrażający zobowiązuje się do prowadzenia postępowań w sprawach o przyznanie lub wypłatę pomocy w zakresie zadań delegowanych, o których mowa w § 2 ust. 2.

§ 8.

Kontrola na miejscu

1. Podmiot wdrażający zobowiązany jest do przeprowadzania kontroli, o których mowa w art. 100 ust. 4 ustawy PS WPR – w zakresie i na poziomie, o których mowa w Wytycznych Ministra Rolnictwa i Rozwoju Wsi w zakresie zasad przeprowadzania kontroli na miejscu w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023-2027. Kontrole na miejscu nie mogą być przeprowadzane przez pracowników, którzy uczestniczyli w kontrolach administracyjnych tej samej operacji.
2. Agencja płatnicza ma prawo weryfikacji poprawności przeprowadzanych przez podmiot wdrażający kontroli na miejscu, zgodnie z trybem wskazanym w § 3 ust. 1 pkt 8 pod względem zgodności z obowiązującymi procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1. Weryfikacja może polegać na kontroli dokumentacji lub wykonywaniu czynności kontrolnych w podmiocie ubiegającym się o przyznanie pomocy / u beneficjenta.

§ 9.

Obowiązki podmiotu wdrażającego w zakresie rozliczeń finansowych

1. Podmiot wdrażający zobowiązuje się do bieżącego przekazywania agencji płatniczej zatwierdzonych do wypłaty zleceń płatności / zleceń korygujących / not korygujących/ dokumentu wstrzymania płatności/ dokumentu cofnięcia wstrzymania z wykorzystaniem wsparcia informatycznego zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.
2. Do zatwierdzonych zleceń płatności / zleceń korygujących, o których mowa w ust. 1, podmiot wdrażający dołącza, z wykorzystaniem wsparcia informatycznego, dokumenty potwierdzające numery rachunków beneficjenta lub cesjonariusza prowadzonych przez banki lub przez spółdzielcze kasy oszczędnościowo-kredytowe, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1, na które agencja płatnicza dokona płatności w ramach Planu Strategicznego, zgodnie z procedurami agencji płatniczej.
3. W przypadku, gdy podmiot wdrażający zatwierdził płatność na kwotę wyższą niż właściwa, a płatność została zrealizowana, podmiot wdrażający zobowiązuje się do przekazania do agencji płatniczej, z wykorzystaniem wsparcia informatycznego, zgłoszenia należności ZW-1, o którym mowa w § 15 ust. 1.
4. Przed podjęciem jakichkolwiek działań skutkujących zmianą kwoty zlecenia płatności przekazanego do agencji płatniczej, a zwłaszcza zmniejszającą tę kwotę, podmiot wdrażający zobowiązuje się przesłać do agencji płatniczej, z wykorzystaniem wsparcia informatycznego, dokumentu o wstrzymaniu realizacji danego zlecenia płatności poprzez wykorzystanie funkcjonalności w systemie IT.
5. Agencja płatnicza dokonuje comiesięcznych uzgodnień z podmiotem wdrażającym danych dotyczących zobowiązań i zrealizowanych płatności na podstawie raportów przekazywanych, z wykorzystaniem wsparcia informatycznego, przez agencję płatniczą do podmiotu wdrażającego.
6. W przypadku stwierdzenia, że beneficjent, którego dotyczy zlecenie płatności przekazane przez podmiot wdrażający widnieje w Rejestrze wykluczonych, agencja płatnicza zwraca zlecenie płatności bez realizacji, wraz z Raportem wstrzymanych zleceń płatności z tytułu rejestracji beneficjentów w Rejestrze wykluczonych w ramach Planu Strategicznego.
7. W przypadku złożenia przez beneficjentów gwarancji lub innych papierów wartościowych stanowiących zabezpieczenie w ramach płatności Planu Strategicznego, podmiot wdrażający wprowadzi je do Rejestru Dokumentów Prawnego Zabezpieczenia, udostępnionego przez agencję płatniczą. W przypadku aneksu lub zwolnienia gwarancji i innych papierów wartościowych podmiot wdrażający niezwłocznie przekaże do agencji płatniczej notę korygującą przy wykorzystaniu funkcjonalności systemu IT oraz wprowadzi do Rejestru aktualne informacje o aneksie lub zwolnieniu wraz ze specyfikacją gwarancji i innych papierów wartościowych.
8. W przypadku otrzymania przez podmiot wdrażający z agencji płatniczej „Zestawienia odrzuconych przez NBP poleceń przelewów” lub „Zestawienia zleceń płatności wstrzymanych, niepobranych do partii płatności” lub „Raportu zwrotów bankowych”, podmiot wdrażający zobowiązuje się, z wykorzystaniem wsparcia informatycznego, do bieżącego przekazywania agencji płatniczej not korygujących do zleceń płatności / zleceń korygujących z wymaganymi załącznikami.
9. Podmiot wdrażający dokonuje z agencją płatniczą uzgodnień stanu ważności przyjętych/ zwolnionych gwarancji/papierów wartościowych stanowiących zabezpieczenie w ramach Planu

Strategicznego, w tym ich okresowej inwentaryzacji, w terminie zgodnym z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.

10. W przypadku, gdy beneficjent zrezygnował z pomocy i rozwiązał umowę o przyznaniu pomocy albo zaistniały inne okoliczności skutkujące rozwiązaniem umowy o przyznaniu pomocy, a zlecenie płatności zostało przekazane do agencji płatniczej celem realizacji, podmiot wdrażający zobowiązuje się niezwłocznie, z wykorzystaniem wsparcia informatycznego, poinformować agencję płatniczą o wstrzymaniu realizacji zlecenia płatności oraz wystawić zlecenie korygujące „in minus".

§ 10.

Obowiązki agencji płatniczej w zakresie realizacji płatności

1. Agencja płatnicza przeprowadza weryfikację formalno-rachunkową przekazywanych przez podmiot wdrażający zatwierdzonych do wypłaty zleceń płatności/zleceń korygujących/not korygujących/dokumentu wstrzymania płatności/dokumentu cofnięcia wstrzymania i załączonych do nich dokumentów w terminie zgodnym z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.
2. Agencja płatnicza przekazuje na rzecz beneficjentów środki finansowe na podstawie przekazanych przez podmiot wdrażający zatwierdzonych do wypłaty zleceń płatności/zleceń korygujących w terminie 5 dni roboczych od daty wpływu na rachunek bankowy agencji płatniczej środków finansowych przeznaczonych na realizacje płatności.
3. Agencja płatnicza informuje podmiot wdrażający, z wykorzystaniem wsparcia informatycznego, o numerze rachunku bankowego, z którego dokonywane będą płatności na rzecz beneficjentów oraz o wszelkich zmianach w numerze tego rachunku.
4. W przypadku, gdy podczas transmisji do NBP poleceń przelewów, NBP nie przyjmie do realizacji poleceń przelewów, z powodu błędnego numeru rachunku bankowego/rachunku prowadzonego w spółdzielczej kasie oszczędnościowo-kredytowej beneficjenta wskazanego w zleceniu płatności, agencja płatnicza przekaże do podmiotu wdrażającego, z wykorzystaniem wsparcia informatycznego, „Zestawienia odrzuconych przez NBP poleceń przelewów".
5. W przypadku, gdy bank beneficjenta lub spółdzielcza kasa oszczędnościowo-kredytowa zwróci agencji płatniczej polecenie przelewu bez realizacji z powodu błędnego numeru rachunku bankowego/ rachunku prowadzonego w spółdzielczej kasie oszczędnościowo-kredytowej beneficjenta wskazanego w zleceniu płatności, agencja płatnicza przekaże do podmiotu wdrażającego, z wykorzystaniem wsparcia informatycznego, „Raport zwrotów bankowych".
6. Agencja płatnicza po dokonaniu płatności na rzecz beneficjentów przekazuje do podmiotu wdrażającego, z wykorzystaniem wsparcia informatycznego, „Zestawienie zrealizowanych płatności" w terminie do 5 dnia roboczego każdego miesiąca następującego po miesiącu, w którym została zrealizowana płatność.

§ 11.

Planowanie wydatków

1. Do dnia 30 grudnia każdego roku podmiot wdrażający przekazuje agencji płatniczej w formie elektronicznej prognozę wydatków w ujęciu kwartalnym na dwa kolejne lata.

2. Do dnia 31 lipca każdego roku podmiot wdrażający przekazuje agencji płatniczej w formie elektronicznej uaktualnioną prognozę wydatków w ujęciu kwartalnym, o której mowa w ust. 1.
3. Podmiot wdrażający sporządza prognozę wydatków w ujęciu miesięcznym obejmującą miesiąc n+1 oraz kolejne miesiące do końca bieżącego roku, którą przekazuje do agencji płatniczej w formie elektronicznej raz w miesiącu do 1-szego dnia roboczego w miesiącu „n".
4. Podmiot wdrażający sporządza założenia do planu wydatkowania środków w ramach realizacji poszczególnych interwencji objętych Planem Strategicznym w ramach EFRROW, w ujęciu kwartalnym na rok n+1, które przekazuje do agencji płatniczej w formie elektronicznej do 30-go dnia miesiąca poprzedzającego rozpoczynający się kwartał, którego dotyczy plan.
5. Podmiot wdrażający sporządza prognozy zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.

§ 12.

Rejestr umów o przyznaniu pomocy oraz aneksów

Podmiot wdrażający zobowiązany jest do prowadzenia w systemie IT udostępnionym przez agencję płatniczą Rejestru zawartych umów o przyznaniu pomocy i aneksów oraz jego bieżącej aktualizacji.

§ 13.

Terminowość realizacji zadań i sprawozdawczość

1. Podmiot wdrażający zobowiązuje się do dotrzymywania terminów weryfikacji wniosków o przyznanie pomocy oraz wniosków o płatność. W przypadku wniosków o płatność podmiot wdrażający zobowiązuje się również do monitorowania terminów ich składania na podstawie danych zawartych w systemie IT.
2. Podmiot wdrażający przygotowuje i przekazuje agencji płatniczej sprawozdania wskazane w procedurach i instrukcjach, o których mowa w § 3 ust. 1 pkt 1, przy pomocy systemu IT.
3. Podmiot wdrażający przygotowuje i przekazuje agencji płatniczej dodatkowe, niezbędne informacje w odniesieniu do realizacji zadań delegowanych w przypadku braku możliwości ich pozyskania z danych będących w posiadaniu agencji płatniczej, w tym z systemu IT, w zakresie i terminie określonym przez agencję płatniczą, przy czym termin ten nie może być krótszy niż 5 dni roboczych, z zastrzeżeniem, że w wyjątkowych przypadkach, po uzgodnieniu z podmiotem wdrażającym termin ten może ulec skróceniu.
4. Przekazywane przez podmiot wdrażający sprawozdania lub tabele monitorowania sporządzane są zgodnie z zaleceniami agencji płatniczej.
5. Podmiot wdrażający zobowiązuje się do przechowywania pozyskanych, zgromadzonych i opracowywanych informacji i danych dotyczących wdrażania Planu Strategicznego, w ramach systemu monitorowania i oceny Planu Strategicznego.
6. Podmiot wdrażający jest zobowiązany do zapewnienia zgodności pomiędzy danymi zawartymi w sprawozdaniach z danymi przechowywanymi w systemie IT.

§ 14.

Wykrywanie, przeciwdziałanie występowaniu nieprawidłowości i nadużyć finansowych oraz ich usuwanie

1. Podmiot wdrażający zobowiązuje się do podjęcia działań w celu wykrywania, przeciwdziałania występowaniu nieprawidłowości i nadużyć finansowych, a w przypadku ich wystąpienia niezwłocznego podejmowania działań w celu ich usunięcia oraz zapobiegania ich ponownemu wystąpieniu, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.
2. Podmiot wdrażający zobowiązuje się, z wykorzystaniem wsparcia informatycznego udostępnionego przez agencję płatniczą, przekazywać do agencji płatniczej informacje o stwierdzonych nieprawidłowościach i nadużyciach finansowych oraz podejrzeniach ich wystąpienia, a także podjętych działaniach w celu ich usunięcia, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1 w zakresie oraz w terminach wymaganych przez agencję płatniczą.
3. Agencja płatnicza monitoruje realizację zadań podmiotu wdrażającego opisanych w ust. 1 i 2 poprzez:
   1) analizę informacji o stwierdzonych nieprawidłowościach i nadużyciach finansowych dostarczanych przez podmiot wdrażający zgodnie z ust. 2;
   2) ocenę podjętych działań w celu usunięcia nieprawidłowości i nadużyć finansowych;
   3) przeprowadzanie kontroli w zakresie wykrywania, przeciwdziałania występowaniu nieprawidłowości i nadużyć finansowych oraz informowania agencji płatniczej o stwierdzonych nieprawidłowościach i nadużyciach finansowych zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1;
   4) zlecanie w uzasadnionych przypadkach służbom kontrolnym podmiotu wdrażającego przeprowadzania dodatkowych czynności dotyczących wykrywania, przeciwdziałania występowaniu nieprawidłowości i nadużyć finansowych oraz informowania agencji płatniczej o stwierdzonych nieprawidłowościach i nadużyciach finansowych w zakresie wymaganym przez agencję płatniczą.

§ 15.

Dochodzenie należności z tytułu środków wypłaconych na podstawie umowy o przyznaniu pomocy

1. Agencja płatnicza dochodzi zwrotu nienależnie lub nadmiernie pobranych środków publicznych na podstawie ustawy o ARiMR, w związku z art. 10 ust. 2 i 3 ustawy PS WPR, po otrzymaniu od podmiotu wdrażającego zgłoszenia należności ZW-1 w zakresie kwot nienależnie lub nadmiernie pobranych środków publicznych ustalonych w drodze decyzji administracyjnej, zgodnie z wymaganymi załącznikami, określonymi w procedurach i instrukcjach, o których mowa w § 3 ust. 1 pkt 1.
2. Podmiot wdrażający zobowiązuje się do przekazania agencji płatniczej dokumentów niezbędnych do dochodzenia zwrotu nienależnie lub nadmiernie pobranych środków publicznych, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.

3. Podmiot wdrażający w terminie 2 dni roboczych przekazuje agencji płatniczej informacje o wniesieniu przez beneficjenta odwołania od decyzji administracyjnej w sprawie ustalenia kwoty nienależnie lub nadmiernie pobranych środków publicznych.
4. Agencja płatnicza w ramach Planu Strategicznego prowadzi „Księgę Dłużników". Wpisanie do „Księgi Dłużników" następuje po otrzymaniu przez agencję płatniczą decyzji ustalającej kwoty nienależnie lub nadmiernie pobranych środków publicznych wraz z poprawnie sporządzonym zgłoszeniem należności ZW-1.
5. W przypadku wykrycia przez agencję płatniczą w zgłoszeniu należności ZW-1 błędów lub braków, agencja płatnicza zwraca się do podmiotu wdrażającego o przekazanie stosownych wyjaśnień, bądź przekazanie poprawnie sporządzonego zgłoszenia należności ZW-1 w terminie 5 dni roboczych od dnia otrzymania zwrotu dokumentu ZW-1.
6. Podmiot wdrażający na wezwanie agencji płatniczej przesyła wskazane przez agencję płatniczą dokumenty niezbędne do prowadzonego postępowania, o którym mowa w § 3 ust. 1 pkt 15.
7. Agencja płatnicza i podmiot wdrażający dokonują comiesięcznego uzgodnienia i weryfikacji spraw wymagających skierowania do dochodzenia zwrotu należności, na zasadach i w terminach wynikających z obowiązujących procedur i instrukcji, o których mowa w § 3 ust. 1 pkt 1.
8. Podmiot wdrażający zobowiązuje się do udzielania odpowiedzi na wystąpienia beneficjentów dotyczące wyjaśnienia przyczyn powstania obowiązku zwrotu całości lub części pomocy oraz jej wysokości z wyjątkiem informacji na temat wysokości naliczonych odsetek.
9. Czynności związane ze zwalnianiem zabezpieczeń wykonuje podmiot wdrażający. W trakcie dochodzenia należności zwolnienie zabezpieczenia następuje na podstawie uzasadnionego wniosku agencji płatniczej przekazanego podmiotowi wdrażającemu wraz z niezbędnymi dokumentami.
10. Agencja płatnicza przekazuje do podmiotu wdrażającego informację o zakończeniu postępowania, o którym mowa w § 3 ust. 1 pkt 15, zgodnie z obowiązującymi procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.

§ 16.

Zarządzanie i kontrola

1. Podmiot wdrażający zapewnia odpowiednią ścieżkę audytu zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.
2. Podmiot wdrażający zobowiązuje się zapewnić organom NIK, KAS, przedstawicielom KE, ETO, agencji płatniczej oraz innym uprawnionym podmiotom dostęp do wszelkich dokumentów odnoszących się do wydatków i płatności dokonanych w związku z realizacją zadań delegowanych, o których mowa w § 2 ust. 2.
3. W zakresie objętym umową podmiot wdrażający zobowiązuje się przygotować do wykonywania zadań delegowanych w sposób, który umożliwi spełnienie przez agencję płatniczą kryteriów akredytacyjnych, określonych w rozporządzeniu 2022/127 jak również prowadzić skuteczny nadzór nad systemem zarządzania i kontroli.
4. Podmiot wdrażający zobowiązuje się do składania „Deklaracji zarządczej" według wzoru przekazanego przez agencję płatniczą, w zakresie prawidłowości realizacji zadań delegowanych, po przeprowadzeniu badania przez służby audytu wewnętrznego podmiotu wdrażającego. Deklaracja składana jest w terminie do dnia 30 listopada (za rolniczy rok budżetowy Unii Europejskiej trwający od 16 października roku n do 15 października roku n+1).

§ 17.

Audyt

1. Pracownicy agencji płatniczej prowadzą w podmiocie wdrażającym czynności audytowe na podstawie imiennego upoważnienia wydanego przez Prezesa agencji płatniczej. Pracownicy agencji płatniczej mogą wykonywać również doraźne czynności audytowe na wniosek Prezesa agencji płatniczej lub z własnej inicjatywy w zakresie z nim uzgodnionym.
2. O zamiarze przeprowadzenia czynności audytowych w podmiocie wdrażającym, kierownik komórki audytu wewnętrznego agencji płatniczej informuje właściwy organ podmiotu wdrażającego w terminie 3 dni roboczych przed rozpoczęciem tych czynności.
3. Upoważnieni pracownicy agencji płatniczej, o których mowa w ust. 1, mogą:
   1) realizować bezpośrednie czynności audytowe w siedzibie podmiotu wdrażającego lub w miejscu wykonywania przez ten podmiot zadań delegowanych;
   2) realizować wszelkie czynności audytowe na odległość, z wykorzystaniem narzędzi komunikacji elektronicznej;
   3) żądać przedstawienia stosownych dokumentów w postaci elektronicznej;
   4) wykonywać, w tym również w postaci elektronicznej, kopie, odpisy oraz wyciągi z dokumentów i innych materiałów związanych z przeprowadzaniem czynności audytowych;
   5) żądać od pracowników podmiotu wdrażającego ustnych i pisemnych wyjaśnień;
   6) prowadzić bezpośrednie czynności audytowe u beneficjentów pomocy w ramach Planu Strategicznego, gdzie podmiot wdrażający był stroną umowy o przyznaniu pomocy.
4. Właściwy organ podmiotu wdrażającego lub osoba upoważniona, zapewnia osobom wskazanym w upoważnieniu, o którym mowa w ust. 1, warunki niezbędne do sprawnego przeprowadzenia audytu.
5. Po przeprowadzeniu czynności audytowych, komórka audytu wewnętrznego agencji płatniczej przedstawia sprawozdanie, w którym w sposób jasny, rzetelny i zwięzły prezentuje wyniki audytu.
6. Kierownik komórki audytu wewnętrznego agencji płatniczej przekazuje sprawozdanie właściwemu organowi podmiotu wdrażającego lub osobie upoważnionej. W przypadku objęcia zakresem zadania kilku podmiotów wdrażających kierownik komórki audytu wewnętrznego agencji płatniczej może przekazać tylko tę część sprawozdania, która dotyczy działalności danego podmiotu wdrażającego.
7. Po otrzymaniu sprawozdania właściwy organ podmiotu wdrażającego lub osoba upoważniona może zgłosić na piśmie dodatkowe wyjaśnienia lub umotywowane zastrzeżenia do treści sprawozdania, w terminie określonym przez kierownika komórki audytu wewnętrznego agencji płatniczej, nie krótszym niż 7 dni roboczych od dnia otrzymania sprawozdania.
8. W przypadku otrzymania dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania, komórka audytu wewnętrznego agencji płatniczej dokonuje ich analizy i w miarę potrzeby podejmuje dodatkowe czynności wyjaśniające w tym zakresie, a w przypadku stwierdzenia w części albo w całości ich zasadności zmienia lub uzupełnia treść sprawozdania. W przypadku nieuwzględnienia dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania, w części albo w całości, kierownik komórki audytu wewnętrznego agencji płatniczej przekazuje na piśmie stanowisko audytu wraz z uzasadnieniem właściwemu organowi podmiotu wdrażającego lub osobie upoważnionej.

9. Po rozpatrzeniu ewentualnych, dodatkowych wyjaśnień lub umotywowanych zastrzeżeń do treści sprawozdania kierownik komórki audytu wewnętrznego agencji płatniczej przekazuje sprawozdanie Prezesowi agencji płatniczej i właściwemu organowi podmiotu wdrażającego lub osobie upoważnionej.
10. Właściwy organ podmiotu wdrażającego lub osoba upoważniona w przypadku uznania, że zalecenia zawarte w sprawozdaniu są zasadne, wyznacza osoby odpowiedzialne za ich realizację oraz ustala sposób i termin ich realizacji, powiadamiając o tym pisemnie kierownika komórki audytu wewnętrznego agencji płatniczej oraz Prezesa agencji płatniczej w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.
11. W przypadku odmowy realizacji zaleceń właściwy organ podmiotu wdrażającego lub osoba upoważniona powiadamia pisemnie kierownika komórki audytu wewnętrznego agencji płatniczej oraz Prezesa agencji płatniczej o przyczynach odmowy w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania.
12. Agencja płatnicza może przeprowadzić czynności sprawdzające, celem dokonania oceny działań podmiotu wdrażającego w zakresie realizacji zaleceń. Ustalenia poczynione w trakcie czynności sprawdzających zamieszczane są w notatce informacyjnej, którą przekazuje kierownik komórki audytu wewnętrznego Prezesowi agencji płatniczej oraz właściwemu organowi podmiotu wdrażającego lub osobie upoważnionej.
13. Podmiot wdrażający zobowiązuje się do:
    1) przeprowadzania co najmniej raz w roku audytów wewnętrznych w zakresie realizacji zadań delegowanych, zgodnie z obowiązującymi przepisami prawa oraz z przyjętymi standardami audytu wewnętrznego;
    2) objęcia zakresem audytów wewnętrznych wszystkich istotnych obszarów związanych z realizacją zadań delegowanych w okresie 5-letnim.
14. Podmiot wdrażający w zakresie zadań powierzonych umową, przekazuje do agencji płatniczej w formie elektronicznej:
    1) roczne plany audytu;
    2) sprawozdania z przeprowadzonego zadania audytowego związanego z realizacją zadań delegowanych, niezwłocznie po zakończeniu danego zadania;
    3) notatki informacyjne z czynności sprawdzających z przeprowadzonego zadania audytowego związanego z realizacją zadań delegowanych, niezwłocznie po zakończeniu czynności sprawdzających;
    4) inne informacje z zakresu realizacji zadań audytowych związanych z realizacją zadań delegowanych, o które wystąpi agencja płatnicza.
15. W uzasadnionych przypadkach, na wniosek agencji płatniczej, podmiot wdrażający zobowiązuje się do przeprowadzenia dodatkowych zadań audytowych w zakresie i terminach wskazanych przez agencję płatniczą.

§ 18.

Monitoring prawidłowości wykonywania przez podmiot wdrażający zadań delegowanych

1. Agencja płatnicza realizuje zadania w zakresie monitoringu prawidłowości wykonywania przez podmiot wdrażający zadań delegowanych, o którym mowa w § 3 ust. 1 pkt 8.
2. Monitoring, o którym mowa w ust. 1, oznacza wszelkie czynności podjęte w celu uzyskania wystarczającej pewności, co do legalności, skuteczności, wydajności, oszczędności i terminowości w realizacji zadań, wiarygodności sprawozdawczości, ochrony informacji, wdrożenia zaleceń / wniosków / rekomendacji, zapobiegania nadużyciom finansowym i nieprawidłowościom, ich wykrywania oraz korygowania i monitorowania.
3. Monitoring, o którym mowa w ust. 1, obejmuje w szczególności sprawdzenie:
   1) prawidłowości i terminowości wykonywania zadań delegowanych, o których mowa w § 2 ust. 2;
   2) przestrzegania i wdrożenia zaleceń / wniosków / rekomendacji, o których mowa w § 3 ust. 2 pkt 21 i 22;
   3) poprawności stosowania przyjętych przez podmiot wdrażający procedur i instrukcji, o których mowa w § 3 ust. 1 pkt 1.
4. Agencja płatnicza pełniąc funkcję gwarancyjną, wynikającą z art. 9 ust. 2 rozporządzenia 2021/2116 ma prawo:
   1) w przypadku powzięcia, przed dokonaniem płatności, uzasadnionych wątpliwości w szczególności w zakresie naruszenia zasad przyznawania lub wypłaty pomocy – wstrzymać realizację zlecenia płatności oraz wezwać podmiot wdrażający do złożenia stosownych wyjaśnień;

      Jeśli agencja płatnicza potwierdzi naruszenie zasad przyznawania lub wypłaty pomocy, nie realizuje płatności, o czym informuje podmiot wdrażający, podając uzasadnienie zajętego stanowiska. W takiej sytuacji podmiot wdrażający zobowiązany jest poinformować beneficjenta o odmowie wypłaty całości lub części pomocy, a w przypadku odmowy wypłaty pomocy w części – wystawić ponownie zlecenie płatności z uwzględnieniem stanowiska agencji płatniczej, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1;
   2) w przypadku powzięcia, po dokonaniu płatności, uzasadnionych wątpliwości w szczególności w zakresie naruszenia zasad przyznawania lub wypłaty pomocy skutkujących wypłatą pomocy nienależnej lub w nadmiernej wysokości – wezwać podmiot wdrażający do złożenia stosownych wyjaśnień;

      Jeśli agencja płatnicza potwierdzi naruszenie zasad przyznawania lub wypłaty pomocy skutkujących wypłatą pomocy nienależnej lub w nadmiernej wysokości, informuje podmiot wdrażający, podając uzasadnienie zajętego stanowiska. W takiej sytuacji podmiot wdrażający zobowiązany jest poinformować beneficjenta o kwocie nienależnie lub nadmiernie pobranych środków publicznych ustalonych w drodze decyzji administracyjnej, następnie wystawić dokument zgłoszenia należności, zgodnie z procedurami i instrukcjami, o których mowa w § 3 ust. 1 pkt 1.

§ 19.

Postanowienia końcowe

1. Niniejsza umowa obowiązuje od dnia zawarcia przez umawiające się Strony do czasu zakończenia realizacji zadań związanych z Planem Strategicznym.
2. Dniem zawarcia umowy jest data złożenia podpisu przez ostatnią ze Stron.
3. Wszelkie zmiany i uzupełnienia treści umowy następują w formie pisemnej, za zgodą Stron umowy, poprzez korespondencyjny obieg dokumentów.
4. W przypadku naruszenia postanowień umowy przez jedną ze Stron, druga Strona ma prawo wypowiedzieć umowę w każdym czasie, z zachowaniem 14-dniowego okresu wypowiedzenia, przy czym wypowiedzenie umowy dla swej skuteczności wymaga formy pisemnej.
5. W przypadku wypowiedzenia umowy przez jedną ze Stron, podmiot wdrażający obowiązany jest przekazać agencji płatniczej pełną dokumentację oraz zbiory danych dotyczące realizacji zadań delegowanych wraz z informacją o stanie realizacji poszczególnych zadań.
6. Wszelkie spory wynikłe pomiędzy Stronami umowy, w związku z wykonaniem umowy, zostaną poddane pod rozstrzygnięcie sądu powszechnego, właściwego według siedziby podmiotu wdrażającego.

Podmiot Wdrażający Agencja Płatnicza

Warunkowa Deklaracja Gotowości

Potwierdzam gotowość do wykonywania przez Samorząd Województwa ……..……..… zadań delegowanych obejmujących w szczególności:

1. prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy, w tym:
   a) przeprowadzanie kontroli administracyjnych,
   b) dokonywanie wyboru operacji oraz w przypadku interwencji I.13.1 Leader/Rozwój Lokalny Kierowany przez Społeczność przeprowadzanie kontroli prawidłowości wyboru operacji w przypadku operacji wybieranych przez Lokalną Grupę Działania,
   c) zawieranie i zmianę umów, na podstawie których jest przyznawana pomoc, informowanie o odmowie jej przyznania i odmowie zawarcia umowy oraz rejestrowanie tych umów i informacji;
2. przeprowadzanie kontroli na miejscu;
3. ustalanie kwot pomocy podlegających zwrotowi i wzywanie beneficjenta do zwrotu tych kwot;
4. przechowywanie dokumentów związanych z wykonywaniem przez Samorząd Województwa zadań Agencji Płatniczej;
5. udostępnianie lub przekazywanie Agencji Płatniczej, Instytucji Zarządzającej, Komisji Europejskiej lub innym organom upoważnionym do kontroli, dokumentów, o których mowa w pkt 4;
6. zatwierdzanie płatności na rzecz beneficjenta;
7. rozpatrywanie środków zaskarżenia na etapie przyznania/wypłaty pomocy finansowej w przypadku interwencji, o których mowa w § 2 pkt 2 ppkt 7 umowy delegowania;
8. prognozowanie wydatków oraz przekazywanie prognoz wydatków do agencji płatniczej w formie elektronicznej, zgodnie z § 11 umowy delegowania zadań Agencji Płatniczej;

oraz poddania się audytowi systemu zarządzania i kontroli przeprowadzanemu przez Agencję Płatniczą w zakresie niżej wymienionych interwencji w ramach PS WPR na lata 2023-2027:

1. *I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym;*
2. *I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi:*
   - Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków,
   - Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś;
3. *I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność* w ramach komponentu:
   - Zarządzanie LSR,
   - Wdrażanie LSR.

Jednocześnie w ramach wykonywania zadań delegowanych przez Agencję Płatniczą potwierdzam, że w Samorządzie Województwa ……. w terminach określonych w Harmonogramie dojścia do osiągnięcia gotowości do wykonywania przez Samorząd Województwa zadań delegowanych przez Agencję Płatniczą w ramach PS WPR na lata 2023 -2027 zostaną spełnione następujące warunki :

1) przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności;
2) wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji, które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;

3) przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023–2027 przekazane do stosowania przez Agencję Płatniczą;
4) zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do Samorządów Województw, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale 6 ustawy PS WPR na lata 2023-2027;
5) bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania" (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.

Potwierdzając gotowość do realizacji zadań delegowanych w zakresie ww. interwencji objętych PS WPR na lata 2023-2027 w ramach przypisanego mi zakresu odpowiedzialności oświadczam, że powyższe jest zgodne ze stanem faktycznym oraz ujawnione zostały wszelkie okoliczności mające wpływ na wydanie niniejszego potwierdzenia gotowości Samorządu Województwa ……

.....	.....
/miejscowość, data/	*/Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023-2027/*
	.....
	Marszałek Województwa

* niepotrzebne skreślić

Harmonogram dojścia do osiągnięcia gotowości do wykonywania przez Samorząd Województwa zadań delegowanych przez Agencję Płatniczą w ramach PS WPR na lata 2023-2027

W ramach PS WPR na lata 2023-2027 dla Interwencji wymienionych w niniejszej Warunkowej Deklaracji Gotowości – Samorząd Województwa …….. przyjmuje następujący Harmonogram dojścia do osiągnięcia gotowości do wykonywania zadań delegowanych przez Agencję Płatniczą:

Zadanie	Podmiot realizujący	Termin
Przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności.	Samorząd Województwa	
Wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje i doświadczenie, które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej.	Samorząd Województwa	
Przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023-2027, przekazane do stosowania przez Agencję płatniczą.	Samorząd Województwa	
Zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do SW, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale u ustawy PS WPR na lata 2023 – 2027.	Samorząd Województwa	
Bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania” (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.	Samorząd Województwa	

…… ……

/miejscowość, data/ */Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023-2027/*

……

Marszałek Województwa

[*] niepotrzebne skreślić

Deklaracja Gotowości

Potwierdzam gotowość do wykonywania przez Samorząd Województwa ……..……..… zadań delegowanych obejmujących w szczególności:

1. prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy, w tym:
   a) przeprowadzanie kontroli administracyjnych,
   b) dokonywanie wyboru operacji oraz w przypadku interwencji I.13.1 Leader/Rozwój Lokalny Kierowany przez Społeczność przeprowadzanie kontroli prawidłowości wyboru operacji w przypadku operacji wybieranych przez Lokalną Grupę Działania,
   c) zawieranie i zmianę umów, na podstawie których jest przyznawana pomoc, informowanie o odmowie jej przyznania i odmowie zawarcia umowy oraz rejestrowanie tych umów i informacji;
2. przeprowadzanie kontroli na miejscu;
3. ustalanie kwot pomocy podlegających zwrotowi i wzywanie beneficjenta do zwrotu tych kwot;
4. przechowywanie dokumentów związanych z wykonywaniem przez Samorząd Województwa zadań Agencji Płatniczej;
5. udostępnianie lub przekazywanie Agencji Płatniczej, Instytucji Zarządzającej, Komisji Europejskiej lub innym organom upoważnionym do kontroli, dokumentów, o których mowa w pkt 4;
6. zatwierdzanie płatności na rzecz beneficjenta;
7. rozpatrywanie środków zaskarżenia na etapie przyznania/wypłaty pomocy finansowej w przypadku interwencji, o których mowa w § 2 pkt 2 ppkt 7 umowy delegowania;
8.
9. prognozowanie wydatków oraz przekazywanie prognoz wydatków do agencji płatniczej w formie elektronicznej, zgodnie z § 11 umowy delegowania zadań Agencji Płatniczej;

oraz poddania się audytowi systemu zarządzania i kontroli przeprowadzanemu przez Agencję Płatniczą w zakresie niżej wymienionych interwencji w ramach PS WPR na lata 2023-2027:

1. *I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym;*
2. *I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi:*
   - Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków,
   - Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś;
3. *I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność* w ramach komponentu:
   - Zarządzanie LSR,
   - Wdrażanie LSR.

Jednocześnie w ramach wykonywania zadań delegowanych przez Agencję Płatniczą potwierdzam, że w Samorządzie Województwa ……. :

1) przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności;
2) wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji , które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;
3) przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023–2027 przekazane do stosowania przez Agencję Płatniczą;

4) zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do Samorządów Województw, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale 6 ustawy PS WPR na lata 2023-2027;
5) bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania” (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.

Potwierdzając gotowość do realizacji zadań delegowanych w zakresie ww. interwencji objętych PS WPR na lata 2023-2027 w ramach przypisanego mi zakresu odpowiedzialności oświadczam, że powyższe jest zgodne ze stanem faktycznym oraz ujawnione zostały wszelkie okoliczności mające wpływ na wydanie niniejszego potwierdzenia gotowości Samorządu Województwa ……..……..…….

.....	.....
miejscowość, data	*Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023 - 2027*
	.....
	Marszałek Województwa

* niepotrzebne skreślić

INSTRUKCJA NADAWANIA ZNAKU SPRAWY

ORAZ NUMERU UMOWY O PRZYZNANIU POMOCY PRZEZ PODMIOTY WDRAŻAJĄCE, KTÓRYM DELEGOWANO ZADANIA AGENCJI PŁATNICZEJ W RAMACH PS WPR NA LATA 2023-2027

1. Informacja ogólna.

Interwencje Planu Strategicznego Wspólnej Polityki Rolnej na lata 2023 -2027 (PS WPR), tzw. zadania delegowane, wdrażane będą przez następujący podmiot wdrażający:

- Samorządy Województw (SW) – w przypadku interwencji:

  I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym

  I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi

  I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność.

Znak sprawy jest stałą cechą rozpoznawczą, na którą składa się zespół symboli alfabetycznych /alfanumerycznych określających przynależność sprawy do określonego podmiotu wdrażającego, hasła kwalifikacyjnego określającego interwencję/komponent interwencji/ rodzaj operacji w ramach PS WPR na lata 2023-2027 oraz numeru, pod którym sprawa została zarejestrowana.

Znak sprawy jest nadawany przez podmiot wdrażający w momencie złożenia przez Wnioskodawcę wniosku o przyznanie pomocy, a w przypadku komponentu Wdrażanie LSR, gdy pomoc udzielana jest wnioskodawcy innemu niż LGD oraz na operacje własne LGD w momencie wpływu do SW wniosków o przyznanie pomocy przekazanych przez LGD.

Dla wniosków o wybór oraz umów o warunkach i sposobie realizacji LSR (umów ramowych) dla tych wniosków, Instrukcja jest stosowana w przypadku, gdy przewidują finansowanie ze środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW) do przyznania pomocy w ramach PS WPR na lata 2023 – 2027.

Każdy dokument sporządzany w trakcie rozpatrywania wniosku, dotyczący tej samej sprawy powinien otrzymać identyczny znak.

Nadanym znakiem sprawy należy również oznaczyć wszelką prowadzoną korespondencję i dokumentację związaną z pomocą. Nie ma wymogu oznaczania znakiem sprawy dokumentów, składanych w ramach uzupełnień, jeśli wykaz tych dokumentów został przekazany wraz z pismem przewodnim, w którym wyszczególniono nazwy tych dokumentów.

2. Symbole klasyfikacyjne.

Symbole klasyfikacyjne, w ramach PS WPR na lata 2023 - 2027 wdrażanych przez podmioty wdrażające, przedstawiają się następująco:

Hasło klasyfikacyjne Rzeczowego Wykazu Akt ARiMR (nazwy interwencji/komponentu interwencji/rodzaju operacji)	**Symbol klasyfikacyjny**
Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	
Wniosek w zakresie interwencji: Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	**65700**
Ewidencja w zakresie interwencji: Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	**65701**
Listy zleceń płatności / zlecenia płatności	**65702**
Infrastruktura na obszarach wiejskich	
Wniosek w zakresie interwencji: Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków	**65710**
Wniosek w zakresie interwencji: Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś	**65711**
Ewidencja w zakresie interwencji: Infrastruktura na obszarach wiejskich	**65712**
Listy zleceń płatności / zlecenia płatności	**65713**
Interwencja: LEADER (Rozwój lokalny kierowany przez społeczność)	
Wybór strategii rozwoju lokalnego kierowanego przez społeczność (LSR)	**6572**
Wniosek w zakresie interwencji: Komponent Zarządzanie LSR	**65720**
Wniosek w zakresie interwencji: Komponent Wdrażanie LSR W tym: 13.1.2.1 – klasyczna operacja 13.1.2.2 – operacje w partnerstwie i projekty partnerskie 13.1.2.3 – operacja własna 13.1.2.4 – projekt grantowy	**65721**
Ewidencja w zakresie interwencji: LEADER (Rozwój lokalny kierowany przez społeczność)	**65722**
Listy zleceń płatności / zlecenia płatności	**65723**
Informacje wyjaśniające w zakresie Interwencji w ramach Planu Strategicznego dla Wspólnej poiltyki Rolnej	**6578**

3. Tworzenie znaku sprawy

Znak sprawy tworzony jest zgodnie ze wzorem:

Dla interwencji:

I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym

I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi

I.13.1 LEADER (Rozwój lokalny kierowany przez społeczność)

LLLL-AAAAA-LLLLKKKKK/RP

gdzie:

LLLL – symbol literowy/numeryczny podmiotu wdrażającego, według poniższego oznaczenia:

UM01 - Urząd Marszałkowski Województwa Dolnośląskiego

UM02 - Urząd Marszałkowski Województwa Kujawsko-Pomorskiego

UM03 - Urząd Marszałkowski Województwa Lubelskiego

UM04 - Urząd Marszałkowski Województwa Lubuskiego

UM05 - Urząd Marszałkowski Województwa Łódzkiego

UM06 - Urząd Marszałkowski Województwa Małopolskiego

UM07 - Urząd Marszałkowski Województwa Mazowieckiego

UM08 - Urząd Marszałkowski Województwa Opolskiego

UM09 - Urząd Marszałkowski Województwa Podkarpackiego

UM10 - Urząd Marszałkowski Województwa Podlaskiego

UM11 - Urząd Marszałkowski Województwa Pomorskiego

UM12 - Urząd Marszałkowski Województwa Śląskiego

UM13 - Urząd Marszałkowski Województwa Świętokrzyskiego

UM14 - Urząd Marszałkowski Województwa Warmińsko-Mazurskiego

UM15 - Urząd Marszałkowski Województwa Wielkopolskiego

UM16 - Urząd Marszałkowski Województwa Zachodniopomorskiego

AAAAA – czterocyfrowy lub pięciocyfrowy symbol klasyfikacyjny według rzeczowego wykazu akt – patrz tabela pkt. 2.

KKKKK – kolejny numer, pod którym sprawa została zarejestrowana w spisie spraw. Numer jest pięciocyfrowy i w razie potrzeby uzupełniany zerami z lewej strony.

RP – dwie ostatnie cyfry roku, w którym powstała sprawa (złożony został wniosek o przyznanie pomocy).

Kolejne numery spraw w ramach danej interwencji/komponentu interwencji/rodzaju operacji powinny być nadawane w sposób ciągły. Początek kolejnego roku kalendarzowego, czy kolejny nabór nie oznaczają, iż w ramach danej interwencji /komponentu interwencji/rodzaju operacji pojawi się sprawa, która będzie miała numer 1. Sprawa powinna otrzymać kolejny numer w spisie spraw (inny niż nr 1).

Postępowanie w przypadkach szczególnych

1) W przypadku konkursu na *Wybór strategii rozwoju lokalnego kierowanego przez społeczność (LSR)*, należy dokonać wyróżnienia typów LSR poprzez dodanie następującej cyfry na początku ciągu KKKKK:

- 1 – w przypadku LSR realizowanej wyłącznie w ramach EFRROW (np. 10001),
- 2 – w przypadku LSR realizowanej przez więcej niż jeden fundusz zgodnie z art. 31 ust. 3 rozporządzenia (UE) 2021/1060 (np. 20001),

2) W przypadku interwencji: *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR*, należy dokonać wyróżnienia rodzajów operacji poprzez dodanie następującej cyfry po kropce na końcu ciągu AAAAA:

- 1 – w przypadku Klasycznej Operacji (np. 0000.1),
- 2 – w przypadku operacji w partnerstwie i projektów partnerskich (np. 0000.2),
- 3 – w przypadku Operacji Własnej (np. 0000.3),
- 4 – w przypadku Projektu Grantowego (np. 0000.4)

Przykłady:

1) Znak sprawy powstałej w 2023 roku, zarejestrowanej w UM Województwa Mazowieckiego w spisie spraw pod numerem 15, w ramach interwencji „*Scalanie gruntów wraz z zagospodarowaniem poscaleniowym*:

   UM07-65700-UM0700015/23

2) Znak sprawy założonej w 2023 roku, zarejestrowanej w UM Województwa Lubelskiego w spisie spraw pod numerem 8, dotyczącej *Wyboru strategii rozwoju lokalnego kierowanego przez społeczność (LSR)* w przypadku LSR realizowanej wyłącznie w ramach EFRROW:

   UM03-6572-UM0310008/23

3) Znak sprawy założonej w 2023 roku, zarejestrowanej w UM Województwa Zachodniopomorskiego w spisie spraw pod numerem 132 w zakresie interwencji: *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR*, operacji w partnerstwie i projektów partnerskich:

   UM16-65721.2-UM1600132/23

4. Tworzenie numeru umowy o przyznaniu pomocy/umowy ramowej

Numer umowy tworzony jest zgodnie ze wzorem:

PPPPP-AAAAA-LLLLKKKKK/RP

gdzie:

PPPPP – znak pięciocyfrowy, unikatowy, przypisany tylko dla jednej umowy tj. kolejny numer umowy w ramach danej interwencji/komponentu interwencji/rodzaju operacji (w ramach danego symbolu klasyfikacyjnego).

Analogicznie jak w przypadku kolejnego numeru znaku sprawy, również kolejne numery umów powinny być nadawane w sposób ciągły, niezależne od roku czy naboru.

AAAAA-LLLLKKKKK/RP – elementy znaku sprawy nadane przy rejestracji wniosku o przyznanie pomocy, patrz pkt 3.

Przykłady:

1) Numer 73 umowy zawartej z Samorządem Województwa Lubuskiego, dla sprawy powstałej w 2023 roku, zarejestrowanej w spisie spraw pod numerem 128, w zakresie interwencji *Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków*

   00073-65710-UM0400128/23

2) Numer 223 umowy zawartej z Samorządem Województwa Opolskiego, dla 158 sprawy założonej w 2023 roku w zakresie interwencji *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR – klasyczna operacja:*

   00223-65721.1-UM0800158/23

3) Numer 14 umowy ramowej zawartej pomiędzy Lokalną Grupą Działania, a Samorządem Województwa Pomorskiego w wyniku konkursu na Wybór strategii

rozwoju lokalnego kierowanego przez społeczność (LSR) w przypadku LSR realizowanej wyłącznie w ramach EFRROW dla sprawy powstałej w 2023 roku zarejestrowanej w spisie spraw pod numerem 17
00014-6572-UM1110017/23

5. Tworzenie numeru umowy o przyznaniu pomocy z Nabywcą przedsiębiorstwa / Następcą prawnym Beneficjenta

Umowa z Nabywcą przedsiębiorstwa / Następcą prawnym Beneficjenta powinna zostać oznaczona numerem zgodnym z numerem umowy zawartej z dotychczasowym beneficjentem, z rozróżnieniem polegającym na dodaniu cyfry 9, jako pierwszej cyfry w pięciocyfrowym oznaczeniu numeru umowy:

9PPPP-AAAAA-LLLLKKKKK/RP

Dokument towarzyszący nr 1
umowie delegowania zadań Agencji Płatniczej do Samorządu Województwa

Warunki organizacyjne, kadrowe i techniczne, jakie powinny spełniać podmioty wdrażające, w związku z wykonywaniem zadań delegowanych przez Agencję płatniczą

Warunki organizacyjne:

1) posiadanie struktury organizacyjnej, adekwatnej do realizacji zadań delegowanych w ramach realizacji Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027, umożliwiającej wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającej wyraźny podział uprawnień i odpowiedzialności, w szczególności posiadanie struktury organizacyjnej zapewniającej prawidłowe wykonywanie czynności kontrolnych oraz przejrzysty podział kompetencji i odpowiedzialności na wszystkich poziomach organizacyjnych;
2) określenie na piśmie obowiązków każdego pracownika, któremu powierzono wykonywanie zadań delegowanych, w szczególności czynności kontrolnych lub zatwierdzanie wyników tych czynności kontrolnych;
3) przyjęcie do stosowania procedur, instrukcji oraz innych dokumentów dotyczących zadań delegowanych, w terminie określonym przez Agencję płatniczą;
4) brak organizacyjnych powiązań z wnioskodawcami / beneficjentami oraz podmiotami kontrolowanymi;
5) zapewnienie wyłączania z realizacji zadań delegowanych, w szczególności czynności kontrolnych, pracowników zatrudnionych w podmiocie wdrażającym, w przypadku wystąpienia przesłanek określonych w art. 24 ustawy Kodeks postępowania administracyjnego lub innych okoliczności mogących wywołać uzasadnione wątpliwości co do ich bezstronności;
6) nie występowanie przesłanek, o których mowa w art. 25 ustawy Kodeks postępowania administracyjnego.

Warunki kadrowe:

1) powierzenie wykonywania zadań pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji które zapewnią ich prawidłowe, rzetelne, bezstronne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;
2) zatrudnianie pracowników wykonujących zadania delegowane, w szczególności czynności kontrolne:
   a) w liczbie zapewniającej samodzielne wykonywanie zadań / czynności i dostosowanej do ich liczby;
   b) posiadających odpowiednie wykształcenie (wyższe lub średnie) i kwalifikacje dostosowane do zakresu powierzonych im zadań lub czynności kontrolnych oraz dające dostateczną wiedzę merytoryczną do wykonywania tych czynności, potwierdzone odpowiednim dokumentem np.: dyplomem, świadectwem, zaświadczeniem, certyfikatem, …;

3) zapewnienie, przed podjęciem realizacji zadań delegowanych, w szczególności czynności kontrolnych, szkoleń pracowników, których odbycie powinno być potwierdzone odpowiednim zaświadczeniem;

4) okresowe sprawdzanie wiedzy w zakresie wprowadzanych zmian w przepisach, procedurach itd. oraz umiejętności pracowników Samorządu Województwa do wykonywania zadań przypisanych do danego stanowiska pracy;

Warunki techniczne:

1) zapewnienie sprzętu pomiarowego:

   a) w liczbie umożliwiającej sprawne wykonywanie czynności kontrolnych, w szczególności pomiarów budowlanych;

   b) umożliwiającego spełnienie wymagań, o których mowa w rozdziale 6 ustawy z dnia 8 lutego 2023 r. o Planie Strategicznym dla Wspólnej Polityki Rolnej na lata 2023–2027;

2) zapewnienie sprzętu informatycznego i oprogramowania spełniającego wymagania techniczne dotyczące przetwarzania i wymiany danych określone przez Agencję płatniczą, o którym mowa w § 4 *Umowy delegowania zadań Agencji Płatniczej*, zgodnie z którego treścią Agencja płatnicza udostępnia nieodpłatnie system IT wspierający realizację zadań delegowanych, w szczególności obejmujący elektroniczny system informacyjny, o którym mowa w art. 130 rozporządzenia (UE) nr 2021/2115 z dnia 2 grudnia 2021 r. ustanawiającego przepisy dotyczące wsparcia planów strategicznych sporządzanych przez państwa członkowskie w ramach wspólnej polityki rolnej (planów strategicznych WPR) i finansowanych z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i z Europejskiego Funduszu Rolnego na Rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz uchylającego rozporządzenia (UE) nr 1305/2013 i (UE) nr 1307/2013, służący do obsługi cyfrowych procesów dla Interwencji Planu Strategicznego;

3) zapewnienie środków transportu i urządzeń telekomunikacyjnych umożliwiających sprawne wykonywanie zadań delegowanych, w szczególności czynności kontrolnych.

Agencja Restrukturyzacji i Modernizacji Rolnictwa
Al. Jana Pawła II nr 70 00-175 Warszawa

Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027

Warszawa, sierpień 2023 r.

Spis treści:

SŁOWNIK TERMINÓW

Występujące w opracowaniu zwroty i skróty oznaczają:

1) **Zalecenia** – niniejszy dokument „Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 20270";
2) **Agencja płatnicza –** Agencja Restrukturyzacji i Modernizacji Rolnictwa;
3) **podmiot wdrażający** – podmiot wykonujący zadania delegowane przez Agencję płatniczą w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 – 2027 czyli Samorząd Województwa, któremu Agencja płatnicza powierzyła wykonywanie tych zadań), realizujący zabezpieczenia zasobów informacyjnych;
4) **Plan Zapewnienia Ciągłości Działania (PZCD)** – plan kontynuowania działalności podmiotu wdrażającego zawierający udokumentowany zbiór procedur i informacji, które są opracowywane, integrowane oraz utrzymywane w gotowości do użycia w sytuacji kryzysowej;
5) **incydent bezpieczeństwa** – zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa informacji, zasobów materialnych lub zdrowia i życia pracowników;
6) **incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub serię zdarzeń niepożądanych lub niespodziewanych związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów biznesowych o istotnym znaczeniu w podmiocie wdrażającym albo ujawnienia informacji posiadających dużą wartość dla podmiotu wdrażającego lub chronionych z mocy prawa;
7) **informacje** – informacje wrażliwe, w tym dane osobowe;
8) **informacja wrażliwa** – informacja prawnie chroniona oraz każda informacja, której utrata, ujawnienie lub udostępnienie osobie / podmiotowi nieuprawnionemu mogłoby spowodować szkodę materialną lub niematerialną dla podmiotu wdrażającego lub naruszyć prawnie chroniony interes innych osób / podmiotów;
9) **Inspektor Bezpieczeństwa Informacji (IBI)** – pracownik pełniący funkcję związaną z nadzorem nad bezpieczeństwem zasobów podmiotu wdrażającego, w tym nad bezpieczeństwem danych osobowych i innych informacji wrażliwych;
10) **użytkownik** – osoba korzystająca z systemu teleinformatycznego Agencji w celu realizacji powierzonych zadań;
11) **logowanie** – proces uwierzytelniania użytkownika w systemie teleinformatycznym udostępnionym przez Agencję płatniczą;
12) **nośnik informacji** – medium magnetyczne, optyczne, półprzewodnikowe lub papierowe, na którym zapisuje się i przechowuje informacje, forma utrwalenia dokumentu;
13) **strefa administracyjna** – obszar, gdzie kontrolowany jest ruch osobowy i materiałowy oraz, do którego dostęp posiadają wszyscy pracownicy podmiotu wdrażającego.

I. OGÓLNE ZASADY WSPÓŁPRACY MIĘDZY AGENCJĄ PŁATNICZĄ A PODMIOTEM WDRAŻAJĄCYM

Podmiot wdrażający zobowiązany jest dostosować bezpieczeństwo informacji – w obszarze przetwarzania danych dotyczących zadań delegowanych na podstawie umowy delegowania zadań Agencji płatniczej do podmiotów wdrażających – do wymagań normy ISO/IEC 27001, z uwzględnieniem niniejszych *Zaleceń*.

Zalecenia przekładają się na następujące zasady współpracy między Agencją płatniczą, a podmiotem wdrażającym:

1. Wytyczne zawarte w Zaleceniach nie zastępują normy: ISO/IEC 27001 stanowią jedynie uzupełnienie wymaganych do wdrożenia i stosowania w obszarze dotyczącym zadań delegowanych norm ISO/IEC 27001.
2. Przyjęty model współpracy zakłada, że podmioty wdrażające korzystają z dostępu do systemu teleinformatycznego udostępnionego przez Agencję płatniczą używając określonych formularzy internetowych (tj. poprzez przeglądarkę internetową).
3. Zawarte w Zaleceniach wytyczne powinny znaleźć odzwierciedlenie w wewnętrznych dokumentach podmiotów wdrażających i być wprowadzone w życie w sposób formalnie przyjęty przez te podmioty.
4. Wymagane jest, aby wdrożenie Zaleceń dotyczących bezpieczeństwa informacji w podmiotach wdrażających odbyło się zgodnie z Harmonogramem dojścia do osiągnięcia gotowości do wykonywania przez podmioty wdrażające zadań delegowanych przez Agencję płatniczą w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027 i znalazło odzwierciedlenie w Deklaracji gotowości lub Warunkowej deklaracji gotowości.

II. NADZÓR NAD BEZPIECZEŃSTWEM INFORMACJI

1. Kierownik podmiotu wdrażającego realizuje nadzór i kontrolę nad bezpieczeństwem informacji, bezpośrednio lub za pośrednictwem wyznaczonego pracownika pełniącego funkcję Inspektora Bezpieczeństwa Informacji (IBI).
2. Czynności kontrolne w ramach nadzoru nad bezpieczeństwem informacji realizowane są w terminach określonych harmonogramem realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowywanym na każdy rok kalendarzowy.
3. Harmonogram realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowuje Inspektor Bezpieczeństwa Informacji w uzgodnieniu z kierownikiem podmiotu wdrażającego lub osobiście kierownik podmiotu wdrażającego.
4. Wskazane jest prowadzenie następujących czynności kontrolnych:
   1) kontrola uprawnień dostępu użytkowników, tj. czy:
      - stosowane są unikalne identyfikatory zgodne z przyjętym schematem;
      - zablokowane zostały wszystkie zbędne identyfikatory (konta użytkowników);
      - przyznane uprawnienia dostępu do systemu teleinformatycznego są zgodne z wnioskiem o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą;
      - przyznane uprawnienia są zgodne z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy;
      - uprawnienia zawarte we wniosku o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą, są zgodne z zakresem upoważnienia do przetwarzania danych osobowych lub innych informacji wrażliwych (jeżeli dotyczy);
      - terminy obowiązywania uprawnień są aktualne;
      - użytkownicy zostali poinformowani o zakresie swoich uprawnień i pisemnie potwierdzili zapoznanie się z nimi;
   2) kontrola wymagań bezpieczeństwa na stanowiskach realizujących zadania delegowane:
      - sprawdzenie, czy dostęp do systemu teleinformatycznego wynikający z realizacji zadań delegowanych jest zgodny z aktualnym zakresem obowiązków pracownika;
   3) kontrola ewidencji osób, którym nadano upoważnienia do przetwarzania danych osobowych, tj. czy:
      - prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych jest kompletna i poprawna;
      - osoby upoważnione zostały przeszkolone z zakresu ochrony danych osobowych i podpisały stosowne oświadczenie.
5. Z każdej kontroli powinien być sporządzony raport.

III. PODSTAWOWE WYMAGANIA I OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU TELEINFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ

A. Szkolenia dla użytkowników systemu teleinformatycznego

1. Warunkiem uzyskania dostępu przez pracownika do systemu teleinformatycznego powinno być odbycie szkolenia z zakresu bezpieczeństwa informacji przeprowadzone przez uprawnionego pracownika podmiotu wdrażającego. Szkolenia użytkowników systemu teleinformatycznego mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić system teleinformatyczny.
2. Okresowo (nie rzadziej niż raz na rok) powinny być przeprowadzane szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia powinny obejmować zagadnienia, które w szczególności dotyczą:
   1) zapoznania użytkowników z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji;
   2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu i aplikacji, itp.);
   3) sposobu postępowania w przypadku zdarzenia (np. incydentu) związanego z naruszeniem bezpieczeństwa informacji;
   4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.

B. Używanie autoryzowanych środków do przetwarzania informacji

1. Każdy środek do przetwarzania informacji powinien podlegać inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym).
2. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
3. Użytkowników obowiązuje zakaz testowania lub podejmowania prób przełamywania zabezpieczeń systemu teleinformatycznego.

C. Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Przez urządzenia przenośne, które mogą służyć do przetwarzania i przechowywania informacji poza siedzibą rozumie się nie tylko wszelkie formy komputerów osobistych, ale także wszelkie rodzaje organizerów, telefonów przenośnych, kart procesorowych i innych rodzajów nośników elektronicznych, magnetycznych i optycznych, używanych do pracy poza biurem podmiotu wdrażającego. Dokumenty papierowe podlegają szczególnej ochronie polegającej na zabezpieczaniu ich przed osobami nieuprawnionymi ze szczególnym uwzględnieniem ich transportu. Dopuszczalna jest praca na dokumentach papierowych poza siedzibą, w wyjątkowych sytuacjach.
2. Dokumenty wydaje się osobom uprawnionym do pracy poza siedzibą za pokwitowaniem. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem. Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.

3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów 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 biurem podmiotu wdrażającego, jeśli pozostają w postaci niezaszyfrowanej.
5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza biurem podmiotu wdrażającego, obowiązany jest do wystąpienia do pracownika bądź komórki odpowiedzialnej za utrzymanie infrastruktury informatycznej z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne oraz ochronę antywirusową.
6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza biurem podmiotu wdrażającego użytkownik niezwłocznie powinien powiadomić o tym fakcie bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłosić ten fakt na policję, traktując jako incydent bezpieczeństwa. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

D. **Korzystanie z systemu teleinformatycznego udostępnionego przez Agencję płatniczą**

1. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
2. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika, na podstawie wniosku o nadanie / zmianę uprawnień, złożonego na wzorze i zgodnie z zasadami określonymi przez Agencję płatniczą.
3. Każdy użytkownik musi posiadać w systemie teleinformatycznym unikalny identyfikator.
4. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
5. W przypadku 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 dostęp do systemu informatycznego.
6. Na stacjach roboczych, na których wykonywane są zadania delegowane, powinno być zabronione m.in.:

1) umożliwianie dostępu do systemu teleinformatycznego osobom nieupoważnionym;
2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika;
3) korzystanie z konta innego użytkownika;
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 systemu teleinformatycznego;
6) samowolnego modyfikowania ustawień związanych z bezpieczeństwem w systemie informatycznym;
7) świadome wprowadzanie błędnych danych do systemu informatycznego;
8) udostępnianie danych osobom nieupoważnionym;
9) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne;
10) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania i danych;
11) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

E. **Ochrona haseł i kluczy kryptograficznych**

1. Hasła użytkowników lub inne dane uwierzytelniające muszą podlegać szczególnej ochronie.
2. Każdy użytkownik systemu teleinformatycznego w podmiocie wdrażającym zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie teleinformatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) poinformowania Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   4) stosowania haseł o minimalnej długości 12 znaków, zawierających kombinację małych i dużych liter oraz cyfr i znaków specjalnych;
   5) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
3. Zabronione powinno być:
   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).
4. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

5. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Inspektorowi Bezpieczeństwa Informacji lub kierownikowi podmiotu wdrażającego.

F. **Zasady „czystego biurka i czystego ekranu”**

1. Podmiot wdrażający powinien prowadzić „politykę czystego biurka i ekranu” obejmującą następujące zasady:
   1) wszelkie dokumenty papierowe i nośniki elektroniczne zawierające dane związane z wykonywaniem zadań delegowanych, kiedy nie są używane, powinny być przechowywane w zamkniętym urządzeniu meblowym (sejf, szafa lub inna forma zabezpieczenia) szczególnie, jeśli w pomieszczeniu biurowym czasowo nie ma pracownika wykonującego te zadania i odpowiadającego za bezpieczeństwo danych;
   2) monitory stacji roboczych należy ustawiać w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu;
   3) komputery osobiste i stacje robocze pozostawiane bez nadzoru lub czasowo nieużywane muszą być wyrejestrowane z sieci lub zablokowane (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub za pomocą innego podobnego mechanizmu);
   4) po zakończeniu pracy należy wylogować się z systemu i wyłączyć komputer; niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia systemu lub przez wyłączenie napięcia zasilającego;
   5) po zakończeniu pracy stanowisko pracy powinno być uporządkowane, w celu uniemożliwienia dostępu osób nieupoważnionych do dokumentów zawierających dane wrażliwe;
   6) punkty przyjmowania i wysyłania korespondencji papierowej winny być odpowiednio zabezpieczone;
   7) w miejscach, gdzie przetwarzane są dane dotyczące zadań delegowanych powinien być wprowadzony zakaz korzystania bez autoryzacji z fotokopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych itp.);
   8) wszelkie wydruki zawierające informacje związane z zadaniami delegowanymi powinny być niezwłocznie usuwane z drukarek, a wydruki uszkodzone natychmiast niszczone w niszczarce dokumentów;
   9) nie należy pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach;
   10) należy przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi lub okien podczas nieobecności w pomieszczeniu.

G. **Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa informacji**

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 m.in.:
   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) pojawianie się nietypowych komunikatów na ekranie;
   7) niemożność zalogowania się do systemu teleinformatycznego;
   8) spowolnienie pracy oprogramowania;
   9) niestabilna praca systemu teleinformatycznego;
   10) brak reakcji systemu na działania użytkownika;
   11) ponowny start lub zawieszanie się komputera;
   12) ograniczenie funkcjonalności oprogramowania.
3. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.
4. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.
5. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędach 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 Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego oraz swojego bezpośredniego przełożonego.

IV. BEZPIECZEŃSTWO FIZYCZNE

1. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego powinien wynikać z przeprowadzonego i udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
   1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.);
   2) określenie kategorii potencjalnych zagrożeń obiektu (wewnętrznych i zewnętrznych) w szczególności pożaru, powodzi, katastrof środowiskowych;
   3) opisu topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące) w szczególności bliskość terenów przemysłowych;
   4) odnotowanych w przeszłości czynów przestępczych (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa);
   5) aktualnego stanu bezpieczeństwa obiektu;
   6) opisu i oceny funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualnego stanu technicznego (poziom technologiczny, sprawność, dokumentacja, serwisowanie);
   7) aktualnego stanu ochrony fizycznej obiektu;
   8) opisu stosowanych procedur i rozwiązań organizacyjnych;
   9) wniosków, co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno–organizacyjnych);
   10) propozycji doskonalenia systemów oraz procedur ochrony obiektu.
3. Za opracowanie oraz stałą aktualizację planu ochrony fizycznej uwzględniającego wyniki szacowania ryzyka winien odpowiadać kierownik podmiotu wdrażającego lub pracownik, któremu powierzono zakres obowiązków związanych z zapewnieniem bezpieczeństwa fizycznego.

A. Obszary bezpieczne

1. Każdy podmiot wdrażający powinien wydzielić z obszaru zajmowanego przez komórki organizacyjne strefę administracyjną i strefę ogólnodostępną. Stacje robocze obsługujące zadania delegowane powinny być zlokalizowane w strefie administracyjnej.
2. Ochrona strefy administracyjnej oraz zastosowane środki bezpieczeństwa powinny być zgodne z zasadami określonymi w ustawie o ochronie osób i mienia i wynikać z opracowanego Planu Ochrony podmiotu wdrażającego.
3. W uzasadnionych przypadkach, gdy czynności związane z realizacją zadań delegowanych muszą być wykonywane przez podmiot wdrażający w ogólnodostępnej strefie, należy dodatkowo przyjąć następujące zasady:

1) strefa administracyjna dla zadań delegowanych może zostać zawężona do miejsc przechowywania bieżącej dokumentacji dotyczącej tych zadań, np. do zamykanych szaf biurowych;
2) stanowiska komputerowe, na których przetwarzane są informacje dotyczące zadań delegowanych powinny:
   - być tak usytuowane, aby uniemożliwić nieuprawnionym osobom przebywającym w pomieszczeniu podgląd danych wyświetlanych na monitorze lub wyprowadzanych na drukarkę;
   - stanowisko powinno być fizycznie wydzielone od pozostałej części pomieszczenia (np. barierką, słupkami i taśmą oddzielającą, itp.);
3) pracownicy w trakcie wykonywania zadań delegowanych odpowiadają bezpośrednio za zabezpieczenie stanowiska komputerowego oraz miejsc przechowywania dokumentacji przed fizycznym dostępem osób trzecich, w tym także przed możliwością podglądu informacji wyświetlanych na ekranie monitora lub drukowanych na drukarce;
4) w przypadku czasowej nieobecności pracownika wykonującego zadania delegowane, stanowisko komputerowe oraz miejsca przechowywania dokumentacji muszą być skutecznie zabezpieczone przed dostępem lub podglądem osób nieupoważnionych;

4. Wykonywanie w ogólnodostępnej strefie zadań delegowanych przez podmiot wdrażający musi być poprzedzone szacowaniem ryzyka i jest dopuszczalne wtedy, gdy poziom ryzyka nie przekracza akceptowalnego poziomu ryzyka.

B. **Zarządzanie kluczami**

1. Klucze wydawać należy na podstawie rejestru osób upoważnionych do ich pobierania, po sprawdzeniu tożsamości osoby pobierającej klucz. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowywany.
2. Za organizację wydawania kluczy do pomieszczeń, w tym za przyznanie i odebranie prawa do ich pobierania, odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
3. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
4. Pozostawanie osób po godzinach służbowych w pracy wymaga, aby spełnione były następujące warunki:
   1) każdy pracownik pozostający po godzinach służbowych w pracy musi mieć wyrażoną zgodę na pozostanie przez kierownika komórki organizacyjnej;
   2) jeśli po godzinach służbowych pozostaje więcej niż jedna osoba, kierownik komórki organizacyjnej (lub urzędu) wyznacza z tej grupy osobę, która będzie odpowiedzialna za właściwe zabezpieczenie obiektu (m.in. uzbrojenie instalacji alarmowej, zamknięcie drzwi wejściowych bądź dopilnowanie tych czynności w przypadku, gdy ktoś inny to wykonuje);

3) jeśli w danym dniu pozostają pracownicy po godzinach służbowych, to obowiązkiem osoby upoważnionej do zabezpieczenia i zamknięcia obiektu po zakończonej pracy, jest pobranie kluczy – na podstawie uzyskanej zgody na pozostanie w pracy.

C. **Lokalizacja oraz ochrona sprzętu i dokumentacji**

1. Środki przetwarzania informacji dotyczącej zadań delegowanych muszą spełniać następujące wymagania bezpieczeństwa:
   1) lokalizacja sprzętu powinna zapewnić minimalizację niepotrzebnego dostępu do obszarów pracy;
   2) lokalizacja środków przetwarzania powinna minimalizować ryzyko podejrzenia przez nieuprawnione osoby, a lokalizacja urządzeń przechowujących informacje zabezpieczać przed nieautoryzowanym dostępem.
2. Pomieszczenia, w których znajdują się szafy do przechowywania dokumentacji dotyczącej zadań delegowanych, powinny posiadać system sygnalizacji pożaru oraz system sygnalizacji włamania.
3. Urządzenia infrastruktury zabezpieczającej muszą być przeglądane i konserwowane zgodnie z instrukcjami i wymaganiami ich producentów.

V. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU ZASOBAMI LUDZKIMI

1. Warunki przystąpienia do pracy, w zależności od zakresu obowiązków, powinny uwzględniać następujące aspekty bezpieczeństwa:
   1) przeszkolenie pracownika w zakresie tematycznym wynikającym z obowiązków i odpowiedzialności na zajmowanym stanowisku;
   2) oświadczenie pracownika o zapoznaniu się z odpowiednimi regulaminami, procedurami i przepisami w sprawie bezpieczeństwa informacji;
   3) przeszkolenie pracownika z zakresu bezpieczeństwa informacji (w tym ochrony danych osobowych), które przeprowadzić należy przed uzyskaniem dostępu do zasobów informacyjnych Agencji płatniczej;
   4) zobowiązanie pracownika do zachowania w poufności informacji wrażliwych, również poza biurem podmiotu wdrażającego i godzinami pracy, a także po ustaniu zatrudnienia bądź zakończeniu wykonywania usług na rzecz podmiotu wdrażającego;
   5) nadanie upoważnienia pracownikowi do przetwarzania danych osobowych.

VI. ZASADY EKSPLOATACJI SYSTEMU TELEINFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ

A. Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery podmiotu wdrażającego powinny być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym.
2. Użytkowane poza systemem podmiotu wdrażającego wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemie teleinformatycznym, należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego.

B. Zasady bezpieczeństwa sieci

1. Sieć informatyczna podmiotu wdrażającego powinna być podłączona do sieci ogólnodostępnych (w szczególności sieci publicznej Internet) przy użyciu specjalnych systemów zabezpieczających, np. aplikacji i urządzeń typu firewall, systemów IDS (Intrusion Detection System) i IPS (Intrusion Prevention System).
2. Reguły filtrowania zapór sieciowych powinny być ustalane i regularnie weryfikowane w zależności od pojawiających się zagrożeń.
3. Wymagania odnoszące się do elementów bezpieczeństwa, poziomu usług i zarządzania wszystkimi usługami sieci muszą być jednoznacznie określone i włączone do odpowiednich umów na dostarczanie tych usług, niezależnie od tego, czy są one częściowo realizowane własnymi środkami, czy zlecane w całości na zewnątrz.

C. Identyfikacja i uwierzytelnianie użytkowników

1. Prawa dostępu do systemu teleinformatycznego przydziela poszczególnym pracownikom podmiotu wdrażającego pracownik pełniący rolę lokalnego administratora podmiotu wdrażającego. Rolę tę nadaje administrator systemu teleinformatycznego Agencji płatniczej. Dostęp do funkcji administracyjnych systemu z poziomu podmiotu wdrażającego jest możliwy tylko dla użytkownika w roli lokalnego administratora podmiotu wdrażającego.
2. Lokalny administrator podmiotu wdrażającego prowadzi rejestr użytkowników z nadanymi uprawnieniami.
3. Do obowiązków lokalnego administratora podmiotu wdrażającego należy także sprawdzanie i blokowanie zbędnych identyfikatorów użytkowników oraz ich kont, aby nie mogły być one wykorzystane powtórnie przez innych użytkowników.
4. Lokalny administrator podmiotu wdrażającego poprzez ustawienia systemowe wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane. Hasło tymczasowe, dostarczane w przypadku, gdy użytkownik zapomni hasła, może być wydane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej.

6. Kontrola praw dostępu użytkowników realizowana jest przez lokalnego administratora podmiotu wdrażającego według następujących zasad:
   1) prawa dostępu użytkowników są przeglądane w regularnych odstępach czasu (nie rzadziej niż co sześć miesięcy) oraz każdorazowo po wprowadzeniu zmian w tych prawach;
   2) w przypadku zmiany miejsca zatrudnienia pracownika, dokonuje się dodatkowego przeglądu i ponownego nadania praw dostępu;
   3) przydzielone uprawnienia są kontrolowane w regularnych odstępach czasu w celu sprawdzenia, czy nie przyznano nadmiarowych uprawnień;
   4) uprawnienia do korzystania ze specjalnie uprzywilejowanych praw dostępu (np. prawa administratora) winny być przeglądane nie rzadziej niż co trzy miesiące;
   5) powinna być prowadzona rejestracja zmian uprzywilejowanych kont na potrzeby okresowych przeglądów;
   6) każde dokonanie kontroli praw dostępu użytkowników powinno zostać udokumentowane sporządzeniem raportu, który należy załączyć do prowadzonej dokumentacji przez lokalnego administratora podmiotu wdrażającego.

D. Zarządzanie wymiennymi nośnikami danych

1. Wymienne nośniki informacji (taśmy, pamięci typu flash, wyjmowane dyski twarde, płyty CD i DVD oraz wydruki) zawierające informacje wrażliwe należy przechowywać w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym.
2. Wszystkie nośniki informacji muszą być przechowywane w bezpiecznym środowisku w warunkach zgodnych z wymaganiami producenta. W przypadku, gdy czas życia nośnika (określony przez producenta) jest krótszy od sumarycznego czasu przechowywania informacji, należy dodatkowo zapewnić, aby na skutek pogorszenia się jakości nośnika nie nastąpiła utrata informacji.
3. Magnetyczne nośniki informacji zawierające kopie bezpieczeństwa oraz informacje archiwalne należy przechowywać w specjalnych, atestowanych, metalowych szafach do przechowywania magnetycznych nośników informacji. Pozostałe nośniki przechowywać i zabezpieczać należy zgodnie z wymaganiami obowiązującymi dla informacji na nich zapisanych.
4. Ograniczać należy do niezbędnego minimum liczby wytwarzanych kopii i wydruków.
5. Zbędne wydruki, notatki, kopie dokumentów, itp. – jeśli zawierają informacje wrażliwe – muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
6. Wszystkie nośniki informacji (taśmy magnetyczne, płyty CD-ROM, wymienne dyski twarde, wydruki komputerowe i inne) wytworzone w systemach informatycznych i zawierające informacje wrażliwe, muszą być ewidencjonowane i oznakowane.
7. Etykiety nośników informacji powinny posiadać identyfikator lub numer umożliwiający ich jednoznaczną klasyfikację i znajdujący odzwierciedlenie w dzienniku ewidencji nośników.

8. Na podstawie etykiety nośnika informacji i danych zawartych w dzienniku ewidencji nośników powinno być możliwe ustalenie:
   1) numeru ewidencyjnego nośnika,
   2) typu nośnika,
   3) daty zapisu na nośniku,
   4) nazwy komórki organizacyjnej składującej informacje,
   5) określenia rodzaju przechowywanej informacji,
   6) imienia i nazwiska osoby dokonującej zapisu.
9. Wycofane nośniki informacji, które były wykorzystywane do przetwarzania informacji wrażliwych, nie mogą być wynoszone poza teren jednostki wdrażającej, w której były użytkowane, bez wcześniejszego skutecznego usunięcia danych.
10. Uszkodzone nośniki, takie jak dyski twarde, i i taśmy magnetyczne, płyty CD-ROM i inne komputerowe nośniki danych, zawierające informacje wrażliwe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji (np. zgniatanie, łamanie, działanie silnym polem magnetycznym).
11. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia powinno być poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.

E. Konserwacja i naprawa sprzętu

1. Sprzęt informatyczny winien podlegać konserwacji według ustalonego planu, wynikającego z zaleceń jego producenta.
2. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawniony personel lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
3. W przypadku, gdy na nośnikach informacji, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje wrażliwe, sprzęt taki naprawiany powinien być pod nadzorem uprawnionego pracownika podmiotu wykonującego zadania delegowane. Jeżeli taki nadzór nie jest możliwy, informacja wrażliwa musi zostać skutecznie usunięta. O ile zachodzi taka możliwość, usuwana informacja powinna być uprzednio zarchiwizowana.
4. Jeżeli gwarant, w ramach naprawy gwarancyjnej, żąda zwrotu urządzenia służącego do przechowywania informacji, informacja wrażliwa znajdująca się w takim urządzeniu musi zostać z niego trwale usunięta. Sposób usuwania danych z nośnika powinny określać szczegółowe procedury.
5. Umowy zawierające gwarancję dostawcy lub producenta muszą zawierać sformułowania umożliwiające realizację postanowień ust. 4 bez utraty gwarancji.
6. W przypadku zbywania sprzętu, bądź przekazywania go do ponownego użycia, należy skutecznie usunąć z niego informacje wrażliwe. Sposób usuwania danych muszą określać szczegółowe procedury.

F. Zarządzanie dostępem do systemu operacyjnego

1. Wszystkie konta użytkowników na stacjach roboczych, na których wykonywane są zadania delegowane, powinny być skonfigurowane z uprawnieniami systemowymi „użytkownik”.
2. Użytkownik systemu operacyjnego powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
4. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
5. Uprawnienia dostępu mogą być nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) powinno być traktowane jako incydent związany z bezpieczeństwem informacji.

VII. OCHRONA DANYCH OSOBOWYCH

1. Kierownik podmiotu wdrażającego wykonuje obowiązki Administratora danych wobec powierzonych mu danych.
2. Kierownik podmiotu wdrażającego odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności, w odniesieniu do wykonywania zadań delegowanych, odpowiada za:
   1) zgodne z prawem (w szczególności z ustawą o ochronie danych osobowych) przetwarzanie danych osobowych;
   2) zapewnienie, aby zgromadzone dane osobowe były merytorycznie poprawne, a ich zakres i rodzaj był adekwatny do celów, w jakich są przetwarzane;
   3) nadawanie upoważnień do przetwarzania danych osobowych;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w, ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
   5) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
3. Upoważnienie do przetwarzania danych osobowych nadaje się przed dopuszczeniem osoby do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych. Upoważnienie odbiera się niezwłocznie po ustaniu celu, dla którego zostało nadane.
4. Upoważnienie do przetwarzania danych osobowych nadawane jest pracownikom, bez względu na podstawę prawną zatrudnienia, po odbyciu szkolenia z ochrony danych osobowych, a fakt odbycia przeszkolenia pracownik powinien potwierdzić podpisując stosowne oświadczenie.

VIII. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA

1. W przypadku, gdy podmiot wdrażający nie posiada planu PZCD, niezbędne jest opracowanie dokumentu, który określi warunki realizacji zadań delegowanych w sytuacji wystąpienia kryzysu. Dokument taki powinien uwzględniać następujące czynniki:
   1) rozpoznanie i uzgodnienie wszystkich procedur awaryjnych i zakresów odpowiedzialności w obszarze zadań delegowanych;
   2) wdrożenie procedur awaryjnych tak, aby umożliwić naprawę i przywrócenie działania w wymaganym czasie z uwzględnieniem zewnętrznych zależności biznesowych (pomiędzy podmiotem wdrażającym a Agencją płatniczą) oraz realizowanych procesów;
   3) dokumentację uzgodnionych procedur oraz procesów operacyjnych i pomocniczych;
   4) przeszkolenie personelu w zakresie uzgodnionych procedur awaryjnych, w tym w zakresie zarządzania w sytuacjach kryzysowych;
   5) procedury awaryjne objęte powyższym dokumentem powinny być przetestowane w roku, w którym uruchomiono realizację zadań delegowanych, a następnie w cyklu rocznym testy winny być powtarzane.
2. Jeśli podmiot wykonujący zadania delegowane opracował i utrzymuje aktualny plan działania PZCD, to do powyższego planu należy włączyć procedury określające sposób postępowania z zadaniami delegowanymi na wypadek wystąpienia kryzysu.

Zasady przepływu informacji dotyczące szczegółowych warunków i trybu przyznawania i zatwierdzania pomocy finansowej oraz stosowania procedur w zakresie zadań delegowanych przez Agencję płatniczą do podmiotów wdrażających w ramach PS WPR na lata 2023 -2027

Słownik

AP	Agencja płatnicza – Agencja Restrukturyzacji i Modernizacji Rolnictwa (ARiMR)
DAiK	Departament Audytu i Kontroli ARiMR
DDD	Departament Działań Delegowanych ARiMR
DBRiKT	Departament Baz Referencyjnych i Kontroli Terenowych ARiMR
DAiS	Departament Analiz i Sprawozdawczości ARiMR
DZN	Departament Zarządzania Należnościami ARiMR
DK	Departament Księgowości ARiMR
DF	Departament Finansowy ARiMR
DPiZP	Departament Prawny i Zamówień Publicznych ARiMR
IZ	Instytucja Zarządzająca – Minister Rolnictwa i Rozwoju Wsi
Departament WPR	Departament Wspólnej Polityki Rolnej w Ministerstwie Rolnictwa i Rozwoju Wsi
PW	Podmiot wdrażający, o którym mowa w art. 2 pkt 22 ustawy z dnia 8 lutego 2023 r. o Planie Strategicznym dla Wspólnej Polityki Rolnej na lata 2023-2027
KP	Książka Procedur
KPH	Książka Procedur Horyzontalna
PS WPR na lata 2023-2027	Plan Strategiczny dla Wspólnej Polityki Rolnej na lata 2023-2027
PUE	Platforma Usług Elektronicznych
System IT	System teleinformatyczny ARiMR, o którym mowa w art. 10 c ustawy o ARiMR z dnia 9 maja 2008 r.
CSOB	Centralny System Obsługi Beneficjenta, który stanowi podstawowe narzędzie obsługi interwencji Planu Strategicznego na lata 2023-2027,

I. Cel

Celem dokumentu jest przyjęcie jednolitych zasad przepływu informacji dotyczących szczegółowych warunków i trybu przyznawania i zatwierdzania pomocy finansowej oraz stosowania procedur w zakresie zadań delegowanych przez AP do PW w ramach PS WPR na lata 2023-2027.

Z uwagi na liczbę podmiotów zaangażowanych w realizację zadań delegowanych istotne jest zapewnienie właściwego i skutecznego systemu komunikacji pomiędzy podmiotami. Pozwoli to uniknąć wydawania wzajemnie wykluczających się stanowisk, nieterminowego przekazywania informacji, nieotrzymania informacji przez wszystkich wymaganych adresatów lub otrzymania ich zbyt późno.

Przygotowanie formalnych zasad komunikacji związane jest w szczególności z koniecznością wypełnienia wymogu akredytacyjnego określonego w załączniku I do rozporządzenia delegowanego Komisji (UE) 2022/127 z dnia 7 grudnia 2021 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/2116 o przepisy dotyczące agencji płatniczych i innych organów, zarządzania finansami, rozliczania rachunków, zabezpieczeń oraz stosowania euro (Dz. Urz. UE L 20 z 31.01.2022, str. 95 z późn. zm.).

Zobowiązanie do stosowania zasad przepływu informacji wynika z postanowień umowy delegowania zadań AP do PW.

II. Zasady ogólne

1. AP jest podmiotem odpowiedzialnym za koordynację przepływu informacji w obszarze zadań delegowanych przez AP, w szczególności za gromadzenie, udostępnianie i przekazywanie informacji w zakresie:
   - szczegółowych warunków i trybu przyznawania oraz zatwierdzania pomocy finansowej,
   - stosowania procedur dotyczących zadań delegowanych przez AP,
   - zmian w zakresie stosowania procedur i instrukcji dotyczących zadań delegowanych przez AP,
   - obsługi systemu IT.

2. Korespondencja pomiędzy AP i PW odbywa się każdorazowo w formie korespondencji elektronicznej lub za pośrednictwem elektronicznej skrzynki podawczej ePUAP.

   W celu usprawnienia przepływu informacji pomiędzy AP i PW możliwe jest wysłanie skanu pisma za pośrednictwem poczty elektronicznej, (zgodnie z listą mailingową).

   Nie ma konieczności wysyłania korespondencji w wersji papierowej, o ile przepisy nie stanowią inaczej.

   Lista mailingowa zostanie utworzona w celu określenia osób odpowiedzialnych za przepływ informacji pomiędzy AP i PW oraz zamieszczona w Chmurze ARiMR.

   Informacja dotycząca adresów poczty elektronicznej wyznaczonych w PW osób – PW przekazują w wersji elektronicznej na adres poczty elektronicznej: delegowane@arimr.gov.pl oraz zamieszczają w Chmurze ARiMR, we wskazanym przez AP katalogu.

   W sytuacji wystąpienia konieczności aktualizacji adresów:

   – PW wysyła informację o aktualizacji na adres poczty elektronicznej: delegowane@arimr.gov.pl, za pośrednictwem poczty elektronicznej i zamieszcza w Chmurze ARiMR, we wskazanym przez AP katalogu.

   – AP wysyła informację o aktualizacji, za pośrednictwem poczty elektronicznej na adresy PW (zgodnie z listą mailingową przekazaną przez PW) i zamieszcza w Chmurze ARiMR, we wskazanym katalogu zaktualizowaną listę mailingową.

   Pisma kierowane do AP powinny być przekazywane w wersji elektronicznej (skan dokumentów) na adres poczty elektronicznej wyznaczonych osób w AP (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027) oraz do wiadomości delegowane@arimr.gov.pl.

   Pismo:

   a. PW zawierające:

   - pytanie w odniesieniu do zadań delegowanych / zagadnień merytorycznych,
   - przekazanie tabeli uwag do dokumentów,

   powinno być podpisane przez upoważnioną osobę w PW (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027).

   b. AP zawierające

   - pytanie / odpowiedź na pytanie PW w odniesieniu do zadań delegowanych / zagadnień merytorycznych,
   - przekazanie dokumentów do opiniowania,

   powinno być podpisane przez upoważnioną osobę w AP (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027).

   Wyjątkiem jest przekazanie KP/KPH do stosowania.

Po uprzednim zatwierdzeniu KP / KPH w AP do PW zostanie przekazana informacja o zatwierdzeniu KP / KPH i obowiązującym terminie przyjęcia jej do stosowania, w postaci papierowej, podpisanej przez Zastępcę Prezesa AP (lub osobę upoważnioną).

Ww. informacja przekazywana jest również na adresy poczty elektronicznej Dyrektorów PW i Departamentu WPR oraz osób wyznaczonych w PW i Departamencie WPR zgodnie z listą mailingową.

3. Jeżeli przygotowanie przez AP stanowiska wymaga interpretacji kwestii generalnych wynikających z przepisów prawa powszechnie obowiązującego, AP występuje do IZ, zgodnie z zasadami występowania przez kierownictwo jednostek nadzorowanych do ministerstwa o interpretację w danym zakresie.

   Podstawę systemu realizacji PS WPR na lata 2023-2027 stanowią jego postanowienia, przepisy prawa powszechnie obowiązującego, Wytyczne IZ oraz regulaminy naborów wniosków.

4. Niniejsze zasady nie obowiązują w sprawach związanych z trybem składania wniosku o przeprowadzenie kontroli doraźnej przez Prezesa Urzędu Zamówień Publicznych.

III. Zasady szczegółowe

1. Przekazywanie pytań

1) Kierowane do AP pytania muszą zawierać:
   a) opis - problemu, zagadnienia, stanu faktycznego,
   b) opinię służb prawnych (jeśli pytanie związane jest z interpretacją przepisów prawa powszechnie obowiązującego),
   c) stanowisko PW w sprawie.

2) PW przekazują wszystkie pytania do AP. Departamentem wiodącym w obszarze zadań delegowanych przez AP jest DDD ARiMR.

3) Jeżeli pytania dotyczą kwestii będących w kompetencjach DBRiKT, DAiK, DZN, DAiS, DK lub DF należy je kierować zgodnie z właściwością:

   – kontrola (kontrola w rozumieniu art. 100 ust. 1 ustawy) oraz stosowanie procedur w tym zakresie – DBRiKT,

   – audyty i ich ustalenia – DAiK,

   – zlecenia zgłoszenia należności (ZW-1 i inne dokumenty towarzyszące) – DZN,

   – monitorowanie i sprawozdawczość oraz stosowanie procedur w tym zakresie – DAiS,

   – dokumenty finansowo-księgowe (zlecenie płatności , korekta zlecenia płatności lub noty) – DK lub DF.

   Pytania należy przesyłać na adresy wyznaczonych osób w AP (zgodnie z kompetencją) oraz do wiadomości DDD, zgodnie z zasadami określonymi w sekcji II pkt. 2.

   Informacja z adresami poczty elektronicznej wyznaczonych osób w AP zostanie przekazana do sekretariatu PW oraz zamieszona w Chmurze ARiMR, we wskazanym przez AP katalogu.

2. Udzielanie odpowiedzi

1) Przygotowanie odpowiedzi AP (DDD).

   Odpowiedzi na pytania przygotowywane są w terminie 30 dni kalendarzowych od wpływu do AP pytania z zastrzeżeniem przypadków, w których odpowiedź zostanie udzielona niezwłocznie po uzgodnieniu stanowiska.

   Jeśli pytania dotyczą również kwestii będących w kompetencjach innych komórek AP lub wymagają konsultacji z innymi komórkami AP, DDD występuje do odpowiedniej komórki o

opinię / stanowisko. Czas na udzielenie odpowiedzi przez DDD w tym przypadku wydłuży się o czas niezbędny na uzyskanie stanowiska z innej komórki ARiMR.

W przypadku, gdy pytanie PW wymaga od AP uzyskania interpretacji kwestii generalnych wynikających z postanowień PS WPR na lata 2023 – 2027, przepisów prawa powszechnie obowiązującego, Wytycznych IZ lub regulaminu naboru wniosków, AP występuje do IZ zgodnie z zasadami występowania przez kierownictwo jednostek nadzorowanych do ministerstwa o interpretację przepisów prawnych.

Ścieżka przekazania pytań do IZ dostosowana jest do obowiązujących zasad przekazywania dokumentów. Pytanie przekazywane jest również w formie skanu dokumentu na adresy elektroniczne Sekretariatu Departamentu WPR oraz osób wyznaczonych w Departamencie WPR.

W przypadku, gdy odpowiedź AP na pytanie PW wymaga od AP uzyskania stanowiska podmiotu zewnętrznego (innego niż IZ), DDD występuje do tego podmiotu o interpretację.

Odpowiedzi w określonej sprawie są przekazywane do PW, który skierował pytanie oraz do wiadomości pozostałych PW, jeśli mogą mieć zastosowanie w sprawach, które dotyczą podobnych zagadnień.

Wydawane stanowiska nie są rozstrzygnięciami AP w indywidualnych sprawach, a jedynie wyjaśnieniem generalnych zasad i mogą być pomocne w ocenie tych spraw.

2) Przygotowanie odpowiedzi AP (komórki inne niż DDD ARiMR).

Opisane w ppkt. 1 zasady dotyczą również odpowiedzi udzielanych przez DBRiKT, DAIK, DZN, DAiS, DK i DF.

Odpowiedzi na pytania przygotowywane przez departamenty inne niż DDD ARiMR są przekazywane do wiadomości DDD ARiMR.

3. Zatwierdzenie lub zmiana formularzy dokumentów aplikacyjnych (wniosków o przyznanie pomocy / wniosków o płatność), umów o przyznaniu pomocy oraz regulaminów naborów (jeśli dotyczy).

AP, przed zatwierdzeniem formularzy, przeprowadzi proces ich uzgodnienia z PW.

W tym celu AP udostępni PW w postaci makiet dokumentów powstałych w systemie IT, formularze dokumentów aplikacyjnych, umów o przyznaniu pomocy oraz regulaminów (jeśli dotyczy), a w sytuacji zaistnienia konieczności zmiany – przygotowuje aktualizację dokumentów.

Formularz umowy o przyznaniu pomocy oraz regulaminu naborów będą udostępniane przez AP jako pliki Word.

Następnie na adresy elektroniczne Dyrektorów PW oraz osób wyznaczonych w PW (zgodnie z listą mailingową) zostanie przekazana przez AP (DDD) informacja o rozpoczęciu konsultacji w zakresie nowych / zmienionych formularzy dokumentów, wraz z podaniem przyczyn zastosowanych zmian.

PW po dokonaniu analizy nowych / zmienionych formularzy przekazuje w terminie wskazanym przez AP, uwagi zgodnie ze wzorem Tabeli uwag zgłaszanych do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naborów /KP/KPH w ramach Interwencji ….. objętego PS WPR na lata 2023 -2027 (wzór tabeli stanowi załącznik nr 1 do niniejszych *Zasad (…)*).

Termin, wskazany w e-mailu AP, może zostać wydłużony na prośbę PW, w zależności od okoliczności w jakich dokonywane jest wprowadzenie lub zmiana formularzy. Informacja o wydłużeniu terminu zostanie przekazana przez AP do wszystkich PW.

Odpowiedź PW na prośbę AP podpisana przez upoważnioną osobę w PW (np. Dyrektor, Zastępca Dyrektora, Kierownik, Naczelnik komórki odpowiedzialnej za realizację PS WPR na lata 2023-2027) przekazywana jest w wersji elektronicznej do Dyrektora DDD i do wiadomości

wyznaczonych osób w AP oraz dodatkowo na adres poczty elektronicznej: delegowane@arimr.gov.pl.

Za przygotowanie zbiorczej *Tabeli zgłaszania uwag do formularza (…)* oraz nadanie statusów uwagom odpowiada AP (DDD). Zbiorcza tabela zostanie przekazana przez AP (DDD) bezzwłocznie do wszystkich PW.

W przypadku uwag o statusie nieuwzględniona lub uwzględniona w części zostanie wskazane przez AP (DDD) uzasadnienie braku możliwości jej uwzględnienia w całości, w części do PW.

Następnie AP(DDD) przeprowadza proces uzgadniania formularzy wewnątrz AP.

AP przekazuje do PW informację o nowym lub zmienionym formularzu oraz obowiązującym terminie jego stosowania (który nie może być wcześniejszy niż data przekazania) na elektroniczną skrzynkę podawczą ePUAP, podpisaną przez Zastępcę Prezesa AP (lub osobę upoważnioną).

Ww. informacja przekazywana jest również na adresy poczty elektronicznej Dyrektorów PW i Departamentu WPR oraz osób wyznaczonych w PW,(zgodnie z listą mailingową) i Departamencie WPR .

Zgłoszenie przez PW do AP (DDD) wad w funkcjonalności formularzy zaimplementowanych w systemie IT możliwe jest każdorazowo, gdy zostaną przez PW wykryte uchybienia.

4. Zatwierdzenie lub zmiana KP / KPH związanych z realizacją zadań delegowanych

AP opracowuje KP / KPH, a w sytuacji zaistnienia konieczności zmiany – wprowadza zmiany do KP / KPH i przygotowuje Kartę aktualizacji a następnie przekazuje do PW informację o rozpoczęciu konsultacji w zakresie nowej / zmienionej KP / KPH. Konsultacje te są prowadzone przed przekazaniem KP / KPH do opiniowania w AP.

Z uwagi na objętość KP / KPH AP zamieści dokumenty do konsultacji jedynie w Chmurze ARiMR (katalog zostanie wskazany w e-mailu z informacją o rozpoczęciu procesu konsultacji).

PW przekazują uwagi do AP, zgodnie ze wzorem *Tabeli zgłaszania uwag zgłaszanych do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naborów / KP/KPH w ramach Interwencji ….. objętego PS WPR na lata 2023 -2027* (wzór tabeli stanowi załącznik nr 1 do niniejszych *Zasad (…)*).

Po dokonanej analizie uwag zgłoszonych przez PW, w tym określeniu statusów do uwag, AP przekaże do PW:

a) wykaz uwag do KP / KPH, który stanowi załącznik nr 2 do niniejszych *Zasad (…)* – w przypadku nowej KP / KPH,
b) kartę aktualizacji do KP / KPH, która stanowi załącznik nr 3 do niniejszych *Zasad (…)* – w przypadku zmiany KP / KPH.

Za przygotowanie zbiorczego zestawienia uwag oraz nadanie statusów odpowiada AP, zgodnie z kompetencjami komórek merytorycznych AP.

Następnie przeprowadzany jest proces zatwierdzania KP / KPH w AP.

Po zatwierdzeniu KP / KPH w AP do PW zostanie przekazana informacja o zatwierdzeniu KP / KPH i obowiązującym terminie przyjęcia jej do stosowania.

Wyznaczony przez AP termin przyjęcia do stosowania KP / KPH nie powinien być krótszy niż 1 miesiąc od dnia przekazania KP / KPH. Możliwe jest skrócenie ww. terminu, po uprzednim uzgodnieniu odpowiednio: ze wszystkimi PW.

Uzgodnienie krótszego niż miesiąc terminu przyjęcia do stosowania KP / KPH, odbywa się poprzez przekazanie przez Dyrektora właściwej komórki AP, na adresy elektroniczne Dyrektorów PW oraz osób wyznaczonych w PW, propozycji AP w tym zakresie oraz otrzymanie informacji zwrotnej od Dyrektorów PW lub upoważnionych osób w PW, również w postaci elektronicznej w terminie 2 dni roboczych od przekazania przez AP propozycji.

Załącznik nr 1

Tabela zgłaszanych uwag do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naboru / KP / KPH [1] w ramach interwencji …….. objętego PS WPR na lata 2023 - 2027

Uwagi do treści zarządzenia					
Uwagi do formularza wniosku o przyznanie pomocy i załączników / instrukcji wypełniania wniosku o przyznanie pomocy / wniosku o płatność i załączników / instrukcji wypełniania wniosku o płatność / umowy o przyznaniu pomocy					
Lp.	Pozycja	Treść dotychczasowa	Uwagi / propozycje zapisu oraz Uzasadnienie	Zgłaszający uwagę	Status

[1] niepotrzebne usunąć

.

Załącznik nr 2

WYKAZ UWAG DO KP / KPH – właściwy symbol klasyfikacyjny RWA-…-ARiMR/…/

Znak sprawy:……..

Lp.	Treść uwagi	Nazwa komórki organizacyjnej zgłaszającej uwagę	Uzasadnienie*
Wykaz wprowadzonych uwag			
1.			
2.			
3.			
Wykaz uwag częściowo uwzględnionych*			
1.			
2.			
3.			
Wykaz uwag nieuwzględnionych*			
1.			
2.			
3.			

Sporządził: ……..……..

(data, imię i nazwisko)

Sprawdził: ……..…….……..

(data, imię i nazwisko)

Zatwierdził: ……..……..

(data, imię i nazwisko)

* W rubryce „Uzasadnienie” AP zamieszcza informację, dlaczego zmiana nie została uwzględniona lub została uwzględniona tylko w części.

Załącznik nr 3

KARTA AKTUALIZACJI KP/KPH

Lp.	Przyczyna zmiany[1]	Miejsce wprowadzenia zmiany[2]	Numer i tytuł KP, na którą ma wpływ proponowana zmiana oraz propozycja zmiany zapisu[3]
1.			
2.			

Sporządził: .....
(data, imię i nazwisko)
Sprawdził: .....
(data, imię i nazwisko)
Zatwierdził: .....
(data, imię i nazwisko)

[1] Należy podać przyczynę zmiany, np. zmiany legislacyjne, zmiany systemu informatycznego, zalecenia audytowe i kontrolne, uwagi komórki organizacyjnej Centrali ARiMR/SW wraz z następującymi informacjami:

- w przypadku, gdy zmiana KP/KPH wynika ze zmiany legislacji należy podać pełną nazwę ustawy, rozporządzenia itp. oraz jednostki redakcyjnej, która wprowadza daną zmianę, tj. art., ust., pkt, lit.;
- w przypadku, gdy zmiana KP/ KPH wynika ze zmiany systemu teleinformatycznego lub istnieje potrzeba modyfikacji systemu IT należy podać numer konkretnego zgłoszenia zmiany do systemu, jeżeli jest nadany numer propozycji lub pisma - wniosku o dokonanie zmiany systemu;
- w przypadku zaleceń audytowych lub kontrolnych należy powołać się na zalecenie (data, strona, treść zalecenia);

w przypadku uwag komórki organizacyjnej Centrali ARiMR/SW należy powołać się na pismo (pismo znak:..., data, treść uwagi)..

[2] Należy podać miejsce wprowadzenia zmiany w przypadku KP/KPH: tj. rozdział, nr strony, regułę, punkt, w przypadku załącznika: nazwę, symbol, nr strony.

[3] Należy podać numer i tytuł KP/KPH, na którą ma wpływ proponowana zmiana. Należy jednoznacznie określić, w jaki sposób proponowana zmiana wpływa na KP/KPH i jakich zmian należy w niej dokonać, w celu zapewnienia spójności między dwoma KP. Jeżeli proponowana zmiana nie ma wpływu na inne KP/KPH, w niniejszej rubryce należy wpisać słowa „zmiana nie ma wpływu na inne KP/KPH”.

Warunkowa Deklaracja Gotowości

Potwierdzam gotowość do wykonywania przez Samorząd Województwa ……..……..… zadań delegowanych obejmujących w szczególności:

1. prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy, w tym:
   a) przeprowadzanie kontroli administracyjnych,
   b) dokonywanie wyboru operacji oraz w przypadku interwencji I.13.1 Leader/Rozwój Lokalny Kierowany przez Społeczność przeprowadzanie kontroli prawidłowości wyboru operacji w przypadku operacji wybieranych przez Lokalną Grupę Działania,
   c) zawieranie i zmianę umów, na podstawie których jest przyznawana pomoc, informowanie o odmowie jej przyznania i odmowie zawarcia umowy oraz rejestrowanie tych umów i informacji;
2. przeprowadzanie kontroli na miejscu;
3. ustalanie kwot pomocy podlegających zwrotowi i wzywanie beneficjenta do zwrotu tych kwot;
4. przechowywanie dokumentów związanych z wykonywaniem przez Samorząd Województwa zadań Agencji Płatniczej;
5. udostępnianie lub przekazywanie Agencji Płatniczej, Instytucji Zarządzającej, Komisji Europejskiej lub innym organom upoważnionym do kontroli, dokumentów, o których mowa w pkt 4;
6. zatwierdzanie płatności na rzecz beneficjenta;
7. rozpatrywanie środków zaskarżenia na etapie przyznania/wypłaty pomocy finansowej w przypadku interwencji, o których mowa w § 2 pkt 2 ppkt 7 umowy delegowania;
8. prognozowanie wydatków oraz przekazywanie prognoz wydatków do agencji płatniczej w formie elektronicznej, zgodnie z § 11 umowy delegowania zadań Agencji Płatniczej;

oraz poddania się audytowi systemu zarządzania i kontroli przeprowadzanemu przez Agencję Płatniczą w zakresie niżej wymienionych interwencji w ramach PS WPR na lata 2023-2027:

1. *I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym;*
2. *I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi:*
   - Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków,
   - Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś;
3. *I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność* w ramach komponentu:
   - Zarządzanie LSR,
   - Wdrażanie LSR.

Jednocześnie w ramach wykonywania zadań delegowanych przez Agencję Płatniczą potwierdzam, że w Samorządzie Województwa ……. w terminach określonych w Harmonogramie dojścia do osiągnięcia gotowości do wykonywania przez Samorząd Województwa zadań delegowanych przez Agencję Płatniczą w ramach PS WPR na lata 2023 -2027 zostaną spełnione następujące warunki :

1) przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności;
2) wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji, które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;

3) przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023–2027 przekazane do stosowania przez Agencję Płatniczą;
4) zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do Samorządów Województw, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale 6 ustawy PS WPR na lata 2023-2027;
5) bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania" (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.

Potwierdzając gotowość do realizacji zadań delegowanych w zakresie ww. interwencji objętych PS WPR na lata 2023-2027 w ramach przypisanego mi zakresu odpowiedzialności oświadczam, że powyższe jest zgodne ze stanem faktycznym oraz ujawnione zostały wszelkie okoliczności mające wpływ na wydanie niniejszego potwierdzenia gotowości Samorządu Województwa ……

.....	.....
/miejscowość, data/	*/Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023-2027/*
	.....
	Marszałek Województwa

* niepotrzebne skreślić

Harmonogram dojścia do osiągnięcia gotowości do wykonywania przez Samorząd Województwa zadań delegowanych przez Agencję Płatniczą w ramach PS WPR na lata 2023-2027

W ramach PS WPR na lata 2023-2027 dla Interwencji wymienionych w niniejszej Warunkowej Deklaracji Gotowości – Samorząd Województwa …….. przyjmuje następujący Harmonogram dojścia do osiągnięcia gotowości do wykonywania zadań delegowanych przez Agencję Płatniczą:

Zadanie	Podmiot realizujący	Termin
Przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności.	Samorząd Województwa	
Wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje i doświadczenie, które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej.	Samorząd Województwa	
Przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023-2027, przekazane do stosowania przez Agencję płatniczą.	Samorząd Województwa	
Zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do SW, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale u ustawy PS WPR na lata 2023 – 2027.	Samorząd Województwa	
Bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania” (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.	Samorząd Województwa	

…… ……

/miejscowość, data/ */Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023-2027/*

……

Marszałek Województwa

[*] niepotrzebne skreślić

Deklaracja Gotowości

Potwierdzam gotowość do wykonywania przez Samorząd Województwa ……..……..… zadań delegowanych obejmujących w szczególności:

1. prowadzenie postępowań w sprawach o przyznanie lub wypłatę pomocy, w tym:
   a) przeprowadzanie kontroli administracyjnych,
   b) dokonywanie wyboru operacji oraz w przypadku interwencji I.13.1 Leader/Rozwój Lokalny Kierowany przez Społeczność przeprowadzanie kontroli prawidłowości wyboru operacji w przypadku operacji wybieranych przez Lokalną Grupę Działania,
   c) zawieranie i zmianę umów, na podstawie których jest przyznawana pomoc, informowanie o odmowie jej przyznania i odmowie zawarcia umowy oraz rejestrowanie tych umów i informacji;
2. przeprowadzanie kontroli na miejscu;
3. ustalanie kwot pomocy podlegających zwrotowi i wzywanie beneficjenta do zwrotu tych kwot;
4. przechowywanie dokumentów związanych z wykonywaniem przez Samorząd Województwa zadań Agencji Płatniczej;
5. udostępnianie lub przekazywanie Agencji Płatniczej, Instytucji Zarządzającej, Komisji Europejskiej lub innym organom upoważnionym do kontroli, dokumentów, o których mowa w pkt 4;
6. zatwierdzanie płatności na rzecz beneficjenta;
7. rozpatrywanie środków zaskarżenia na etapie przyznania/wypłaty pomocy finansowej w przypadku interwencji, o których mowa w § 2 pkt 2 ppkt 7 umowy delegowania;
8.
9. prognozowanie wydatków oraz przekazywanie prognoz wydatków do agencji płatniczej w formie elektronicznej, zgodnie z § 11 umowy delegowania zadań Agencji Płatniczej;

oraz poddania się audytowi systemu zarządzania i kontroli przeprowadzanemu przez Agencję Płatniczą w zakresie niżej wymienionych interwencji w ramach PS WPR na lata 2023-2027:

1. *I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym;*
2. *I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi:*
   - Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków,
   - Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś;
3. *I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność* w ramach komponentu:
   - Zarządzanie LSR,
   - Wdrażanie LSR.

Jednocześnie w ramach wykonywania zadań delegowanych przez Agencję Płatniczą potwierdzam, że w Samorządzie Województwa ……. :

1) przyjęto strukturę organizacyjną, adekwatną do realizacji zadań delegowanych w ramach perspektywy finansowej 2023-2027, umożliwiającą wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającą wyraźny podział uprawnień i odpowiedzialności;
2) wykonywanie zadań powierzono pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji , które zapewnią ich prawidłowe, rzetelne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;
3) przyjęto procedury, instrukcje postępowania związane z realizacją zadań delegowanych, łącznie z opisem dokumentów, którymi należy się posługiwać w ramach perspektywy finansowej 2023–2027 przekazane do stosowania przez Agencję Płatniczą;

4) zapewniono właściwe warunki organizacyjne, kadrowe i techniczne wykonywania zadań delegowanych do Samorządów Województw, w szczególności w zakresie służb wykonujących kontrole, o których mowa w rozdziale 6 ustawy PS WPR na lata 2023-2027;
5) bezpieczeństwo systemów informacyjnych opiera się na kryteriach określonych w normie Międzynarodowej Organizacji Normalizacyjnej 27001: „System zarządzania bezpieczeństwem informacji – Wymagania” (ISO) – zgodnie z przepisami rozporządzenia delegowanego Komisji (UE) 2022/127.

Potwierdzając gotowość do realizacji zadań delegowanych w zakresie ww. interwencji objętych PS WPR na lata 2023-2027 w ramach przypisanego mi zakresu odpowiedzialności oświadczam, że powyższe jest zgodne ze stanem faktycznym oraz ujawnione zostały wszelkie okoliczności mające wpływ na wydanie niniejszego potwierdzenia gotowości Samorządu Województwa ……..……..…….

.....	.....
miejscowość, data	*Dyrektor / Kierownik komórki odpowiedzialnej za wdrażanie zadań delegowanych w ramach PS WPR na lata 2023 - 2027*
	.....
	Marszałek Województwa

* niepotrzebne skreślić

INSTRUKCJA NADAWANIA ZNAKU SPRAWY

ORAZ NUMERU UMOWY O PRZYZNANIU POMOCY PRZEZ PODMIOTY WDRAŻAJĄCE, KTÓRYM DELEGOWANO ZADANIA AGENCJI PŁATNICZEJ W RAMACH PS WPR NA LATA 2023-2027

1. Informacja ogólna.

Interwencje Planu Strategicznego Wspólnej Polityki Rolnej na lata 2023 -2027 (PS WPR), tzw. zadania delegowane, wdrażane będą przez następujący podmiot wdrażający:

- Samorządy Województw (SW) – w przypadku interwencji:

  I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym

  I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi

  I.13.1 LEADER/Rozwój lokalny kierowany przez społeczność.

Znak sprawy jest stałą cechą rozpoznawczą, na którą składa się zespół symboli alfabetycznych /alfanumerycznych określających przynależność sprawy do określonego podmiotu wdrażającego, hasła kwalifikacyjnego określającego interwencję/komponent interwencji/ rodzaj operacji w ramach PS WPR na lata 2023-2027 oraz numeru, pod którym sprawa została zarejestrowana.

Znak sprawy jest nadawany przez podmiot wdrażający w momencie złożenia przez Wnioskodawcę wniosku o przyznanie pomocy, a w przypadku komponentu Wdrażanie LSR, gdy pomoc udzielana jest wnioskodawcy innemu niż LGD oraz na operacje własne LGD w momencie wpływu do SW wniosków o przyznanie pomocy przekazanych przez LGD.

Dla wniosków o wybór oraz umów o warunkach i sposobie realizacji LSR (umów ramowych) dla tych wniosków, Instrukcja jest stosowana w przypadku, gdy przewidują finansowanie ze środków Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW) do przyznania pomocy w ramach PS WPR na lata 2023 – 2027.

Każdy dokument sporządzany w trakcie rozpatrywania wniosku, dotyczący tej samej sprawy powinien otrzymać identyczny znak.

Nadanym znakiem sprawy należy również oznaczyć wszelką prowadzoną korespondencję i dokumentację związaną z pomocą. Nie ma wymogu oznaczania znakiem sprawy dokumentów, składanych w ramach uzupełnień, jeśli wykaz tych dokumentów został przekazany wraz z pismem przewodnim, w którym wyszczególniono nazwy tych dokumentów.

2. Symbole klasyfikacyjne.

Symbole klasyfikacyjne, w ramach PS WPR na lata 2023 - 2027 wdrażanych przez podmioty wdrażające, przedstawiają się następująco:

Hasło klasyfikacyjne Rzeczowego Wykazu Akt ARiMR (nazwy interwencji/komponentu interwencji/rodzaju operacji)	**Symbol klasyfikacyjny**
Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	
Wniosek w zakresie interwencji: Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	**65700**
Ewidencja w zakresie interwencji: Scalanie gruntów wraz z zagospodarowaniem poscaleniowym	**65701**
Listy zleceń płatności / zlecenia płatności	**65702**
Infrastruktura na obszarach wiejskich	
Wniosek w zakresie interwencji: Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków	**65710**
Wniosek w zakresie interwencji: Infrastruktura na obszarach wiejskich – Obszar B Inteligentna wieś	**65711**
Ewidencja w zakresie interwencji: Infrastruktura na obszarach wiejskich	**65712**
Listy zleceń płatności / zlecenia płatności	**65713**
Interwencja: LEADER (Rozwój lokalny kierowany przez społeczność)	
Wybór strategii rozwoju lokalnego kierowanego przez społeczność (LSR)	**6572**
Wniosek w zakresie interwencji: Komponent Zarządzanie LSR	**65720**
Wniosek w zakresie interwencji: Komponent Wdrażanie LSR W tym: 13.1.2.1 – klasyczna operacja 13.1.2.2 – operacje w partnerstwie i projekty partnerskie 13.1.2.3 – operacja własna 13.1.2.4 – projekt grantowy	**65721**
Ewidencja w zakresie interwencji: LEADER (Rozwój lokalny kierowany przez społeczność)	**65722**
Listy zleceń płatności / zlecenia płatności	**65723**
Informacje wyjaśniające w zakresie Interwencji w ramach Planu Strategicznego dla Wspólnej poiltyki Rolnej	**6578**

3. Tworzenie znaku sprawy

Znak sprawy tworzony jest zgodnie ze wzorem:

Dla interwencji:

I.10.8 Scalanie gruntów wraz z zagospodarowaniem poscaleniowym

I.10.10 Infrastruktura na obszarach wiejskich oraz wdrożenie koncepcji inteligentnych wsi

I.13.1 LEADER (Rozwój lokalny kierowany przez społeczność)

LLLL-AAAAA-LLLLKKKKK/RP

gdzie:

LLLL – symbol literowy/numeryczny podmiotu wdrażającego, według poniższego oznaczenia:

UM01 - Urząd Marszałkowski Województwa Dolnośląskiego

UM02 - Urząd Marszałkowski Województwa Kujawsko-Pomorskiego

UM03 - Urząd Marszałkowski Województwa Lubelskiego

UM04 - Urząd Marszałkowski Województwa Lubuskiego

UM05 - Urząd Marszałkowski Województwa Łódzkiego

UM06 - Urząd Marszałkowski Województwa Małopolskiego

UM07 - Urząd Marszałkowski Województwa Mazowieckiego

UM08 - Urząd Marszałkowski Województwa Opolskiego

UM09 - Urząd Marszałkowski Województwa Podkarpackiego

UM10 - Urząd Marszałkowski Województwa Podlaskiego

UM11 - Urząd Marszałkowski Województwa Pomorskiego

UM12 - Urząd Marszałkowski Województwa Śląskiego

UM13 - Urząd Marszałkowski Województwa Świętokrzyskiego

UM14 - Urząd Marszałkowski Województwa Warmińsko-Mazurskiego

UM15 - Urząd Marszałkowski Województwa Wielkopolskiego

UM16 - Urząd Marszałkowski Województwa Zachodniopomorskiego

AAAAA – czterocyfrowy lub pięciocyfrowy symbol klasyfikacyjny według rzeczowego wykazu akt – patrz tabela pkt. 2.

KKKKK – kolejny numer, pod którym sprawa została zarejestrowana w spisie spraw. Numer jest pięciocyfrowy i w razie potrzeby uzupełniany zerami z lewej strony.

RP – dwie ostatnie cyfry roku, w którym powstała sprawa (złożony został wniosek o przyznanie pomocy).

Kolejne numery spraw w ramach danej interwencji/komponentu interwencji/rodzaju operacji powinny być nadawane w sposób ciągły. Początek kolejnego roku kalendarzowego, czy kolejny nabór nie oznaczają, iż w ramach danej interwencji /komponentu interwencji/rodzaju operacji pojawi się sprawa, która będzie miała numer 1. Sprawa powinna otrzymać kolejny numer w spisie spraw (inny niż nr 1).

Postępowanie w przypadkach szczególnych

1) W przypadku konkursu na *Wybór strategii rozwoju lokalnego kierowanego przez społeczność (LSR)*, należy dokonać wyróżnienia typów LSR poprzez dodanie następującej cyfry na początku ciągu KKKKK:

- 1 – w przypadku LSR realizowanej wyłącznie w ramach EFRROW (np. 10001),
- 2 – w przypadku LSR realizowanej przez więcej niż jeden fundusz zgodnie z art. 31 ust. 3 rozporządzenia (UE) 2021/1060 (np. 20001),

2) W przypadku interwencji: *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR*, należy dokonać wyróżnienia rodzajów operacji poprzez dodanie następującej cyfry po kropce na końcu ciągu AAAAA:

- 1 – w przypadku Klasycznej Operacji (np. 0000.1),
- 2 – w przypadku operacji w partnerstwie i projektów partnerskich (np. 0000.2),
- 3 – w przypadku Operacji Własnej (np. 0000.3),
- 4 – w przypadku Projektu Grantowego (np. 0000.4)

Przykłady:

1) Znak sprawy powstałej w 2023 roku, zarejestrowanej w UM Województwa Mazowieckiego w spisie spraw pod numerem 15, w ramach interwencji „*Scalanie gruntów wraz z zagospodarowaniem poscaleniowym*:

   UM07-65700-UM0700015/23

2) Znak sprawy założonej w 2023 roku, zarejestrowanej w UM Województwa Lubelskiego w spisie spraw pod numerem 8, dotyczącej *Wyboru strategii rozwoju lokalnego kierowanego przez społeczność (LSR)* w przypadku LSR realizowanej wyłącznie w ramach EFRROW:

   UM03-6572-UM0310008/23

3) Znak sprawy założonej w 2023 roku, zarejestrowanej w UM Województwa Zachodniopomorskiego w spisie spraw pod numerem 132 w zakresie interwencji: *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR*, operacji w partnerstwie i projektów partnerskich:

   UM16-65721.2-UM1600132/23

4. Tworzenie numeru umowy o przyznaniu pomocy/umowy ramowej

Numer umowy tworzony jest zgodnie ze wzorem:

PPPPP-AAAAA-LLLLKKKKK/RP

gdzie:

PPPPP – znak pięciocyfrowy, unikatowy, przypisany tylko dla jednej umowy tj. kolejny numer umowy w ramach danej interwencji/komponentu interwencji/rodzaju operacji (w ramach danego symbolu klasyfikacyjnego).

Analogicznie jak w przypadku kolejnego numeru znaku sprawy, również kolejne numery umów powinny być nadawane w sposób ciągły, niezależne od roku czy naboru.

AAAAA-LLLLKKKKK/RP – elementy znaku sprawy nadane przy rejestracji wniosku o przyznanie pomocy, patrz pkt 3.

Przykłady:

1) Numer 73 umowy zawartej z Samorządem Województwa Lubuskiego, dla sprawy powstałej w 2023 roku, zarejestrowanej w spisie spraw pod numerem 128, w zakresie interwencji *Infrastruktura na obszarach wiejskich – Obszar A Inwestycje w zakresie indywidualnego oczyszczania ścieków*

   00073-65710-UM0400128/23

2) Numer 223 umowy zawartej z Samorządem Województwa Opolskiego, dla 158 sprawy założonej w 2023 roku w zakresie interwencji *LEADER (Rozwój lokalny kierowany przez społeczność) – komponent Wdrażanie LSR – klasyczna operacja:*

   00223-65721.1-UM0800158/23

3) Numer 14 umowy ramowej zawartej pomiędzy Lokalną Grupą Działania, a Samorządem Województwa Pomorskiego w wyniku konkursu na Wybór strategii

rozwoju lokalnego kierowanego przez społeczność (LSR) w przypadku LSR realizowanej wyłącznie w ramach EFRROW dla sprawy powstałej w 2023 roku zarejestrowanej w spisie spraw pod numerem 17
00014-6572-UM1110017/23

5. Tworzenie numeru umowy o przyznaniu pomocy z Nabywcą przedsiębiorstwa / Następcą prawnym Beneficjenta

Umowa z Nabywcą przedsiębiorstwa / Następcą prawnym Beneficjenta powinna zostać oznaczona numerem zgodnym z numerem umowy zawartej z dotychczasowym beneficjentem, z rozróżnieniem polegającym na dodaniu cyfry 9, jako pierwszej cyfry w pięciocyfrowym oznaczeniu numeru umowy:

9PPPP-AAAAA-LLLLKKKKK/RP

Dokument towarzyszący nr 1
umowie delegowania zadań Agencji Płatniczej do Samorządu Województwa

Warunki organizacyjne, kadrowe i techniczne, jakie powinny spełniać podmioty wdrażające, w związku z wykonywaniem zadań delegowanych przez Agencję płatniczą

Warunki organizacyjne:

1) posiadanie struktury organizacyjnej, adekwatnej do realizacji zadań delegowanych w ramach realizacji Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027, umożliwiającej wykonywanie głównych zadań w odniesieniu do wydatków EFRROW, zapewniającej wyraźny podział uprawnień i odpowiedzialności, w szczególności posiadanie struktury organizacyjnej zapewniającej prawidłowe wykonywanie czynności kontrolnych oraz przejrzysty podział kompetencji i odpowiedzialności na wszystkich poziomach organizacyjnych;
2) określenie na piśmie obowiązków każdego pracownika, któremu powierzono wykonywanie zadań delegowanych, w szczególności czynności kontrolnych lub zatwierdzanie wyników tych czynności kontrolnych;
3) przyjęcie do stosowania procedur, instrukcji oraz innych dokumentów dotyczących zadań delegowanych, w terminie określonym przez Agencję płatniczą;
4) brak organizacyjnych powiązań z wnioskodawcami / beneficjentami oraz podmiotami kontrolowanymi;
5) zapewnienie wyłączania z realizacji zadań delegowanych, w szczególności czynności kontrolnych, pracowników zatrudnionych w podmiocie wdrażającym, w przypadku wystąpienia przesłanek określonych w art. 24 ustawy Kodeks postępowania administracyjnego lub innych okoliczności mogących wywołać uzasadnione wątpliwości co do ich bezstronności;
6) nie występowanie przesłanek, o których mowa w art. 25 ustawy Kodeks postępowania administracyjnego.

Warunki kadrowe:

1) powierzenie wykonywania zadań pracownikom posiadającym odpowiednie kwalifikacje lub doświadczenie oraz odpowiednie przeszkolenie z procedur i instrukcji które zapewnią ich prawidłowe, rzetelne, bezstronne, sprawne i terminowe wykonanie, a ich zakresy obowiązków określono w formie pisemnej;
2) zatrudnianie pracowników wykonujących zadania delegowane, w szczególności czynności kontrolne:
   a) w liczbie zapewniającej samodzielne wykonywanie zadań / czynności i dostosowanej do ich liczby;
   b) posiadających odpowiednie wykształcenie (wyższe lub średnie) i kwalifikacje dostosowane do zakresu powierzonych im zadań lub czynności kontrolnych oraz dające dostateczną wiedzę merytoryczną do wykonywania tych czynności, potwierdzone odpowiednim dokumentem np.: dyplomem, świadectwem, zaświadczeniem, certyfikatem, …;

3) zapewnienie, przed podjęciem realizacji zadań delegowanych, w szczególności czynności kontrolnych, szkoleń pracowników, których odbycie powinno być potwierdzone odpowiednim zaświadczeniem;

4) okresowe sprawdzanie wiedzy w zakresie wprowadzanych zmian w przepisach, procedurach itd. oraz umiejętności pracowników Samorządu Województwa do wykonywania zadań przypisanych do danego stanowiska pracy;

Warunki techniczne:

1) zapewnienie sprzętu pomiarowego:

   a) w liczbie umożliwiającej sprawne wykonywanie czynności kontrolnych, w szczególności pomiarów budowlanych;

   b) umożliwiającego spełnienie wymagań, o których mowa w rozdziale 6 ustawy z dnia 8 lutego 2023 r. o Planie Strategicznym dla Wspólnej Polityki Rolnej na lata 2023–2027;

2) zapewnienie sprzętu informatycznego i oprogramowania spełniającego wymagania techniczne dotyczące przetwarzania i wymiany danych określone przez Agencję płatniczą, o którym mowa w § 4 *Umowy delegowania zadań Agencji Płatniczej*, zgodnie z którego treścią Agencja płatnicza udostępnia nieodpłatnie system IT wspierający realizację zadań delegowanych, w szczególności obejmujący elektroniczny system informacyjny, o którym mowa w art. 130 rozporządzenia (UE) nr 2021/2115 z dnia 2 grudnia 2021 r. ustanawiającego przepisy dotyczące wsparcia planów strategicznych sporządzanych przez państwa członkowskie w ramach wspólnej polityki rolnej (planów strategicznych WPR) i finansowanych z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i z Europejskiego Funduszu Rolnego na Rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz uchylającego rozporządzenia (UE) nr 1305/2013 i (UE) nr 1307/2013, służący do obsługi cyfrowych procesów dla Interwencji Planu Strategicznego;

3) zapewnienie środków transportu i urządzeń telekomunikacyjnych umożliwiających sprawne wykonywanie zadań delegowanych, w szczególności czynności kontrolnych.

Agencja Restrukturyzacji i Modernizacji Rolnictwa
Al. Jana Pawła II nr 70 00-175 Warszawa

Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027

Warszawa, sierpień 2023 r.

Spis treści:

SŁOWNIK TERMINÓW

Występujące w opracowaniu zwroty i skróty oznaczają:

1) **Zalecenia** – niniejszy dokument „Zalecenia dla podmiotów wdrażających realizujących zadania delegowane w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 20270";
2) **Agencja płatnicza –** Agencja Restrukturyzacji i Modernizacji Rolnictwa;
3) **podmiot wdrażający** – podmiot wykonujący zadania delegowane przez Agencję płatniczą w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 – 2027 czyli Samorząd Województwa, któremu Agencja płatnicza powierzyła wykonywanie tych zadań), realizujący zabezpieczenia zasobów informacyjnych;
4) **Plan Zapewnienia Ciągłości Działania (PZCD)** – plan kontynuowania działalności podmiotu wdrażającego zawierający udokumentowany zbiór procedur i informacji, które są opracowywane, integrowane oraz utrzymywane w gotowości do użycia w sytuacji kryzysowej;
5) **incydent bezpieczeństwa** – zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa informacji, zasobów materialnych lub zdrowia i życia pracowników;
6) **incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub serię zdarzeń niepożądanych lub niespodziewanych związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów biznesowych o istotnym znaczeniu w podmiocie wdrażającym albo ujawnienia informacji posiadających dużą wartość dla podmiotu wdrażającego lub chronionych z mocy prawa;
7) **informacje** – informacje wrażliwe, w tym dane osobowe;
8) **informacja wrażliwa** – informacja prawnie chroniona oraz każda informacja, której utrata, ujawnienie lub udostępnienie osobie / podmiotowi nieuprawnionemu mogłoby spowodować szkodę materialną lub niematerialną dla podmiotu wdrażającego lub naruszyć prawnie chroniony interes innych osób / podmiotów;
9) **Inspektor Bezpieczeństwa Informacji (IBI)** – pracownik pełniący funkcję związaną z nadzorem nad bezpieczeństwem zasobów podmiotu wdrażającego, w tym nad bezpieczeństwem danych osobowych i innych informacji wrażliwych;
10) **użytkownik** – osoba korzystająca z systemu teleinformatycznego Agencji w celu realizacji powierzonych zadań;
11) **logowanie** – proces uwierzytelniania użytkownika w systemie teleinformatycznym udostępnionym przez Agencję płatniczą;
12) **nośnik informacji** – medium magnetyczne, optyczne, półprzewodnikowe lub papierowe, na którym zapisuje się i przechowuje informacje, forma utrwalenia dokumentu;
13) **strefa administracyjna** – obszar, gdzie kontrolowany jest ruch osobowy i materiałowy oraz, do którego dostęp posiadają wszyscy pracownicy podmiotu wdrażającego.

I. OGÓLNE ZASADY WSPÓŁPRACY MIĘDZY AGENCJĄ PŁATNICZĄ A PODMIOTEM WDRAŻAJĄCYM

Podmiot wdrażający zobowiązany jest dostosować bezpieczeństwo informacji – w obszarze przetwarzania danych dotyczących zadań delegowanych na podstawie umowy delegowania zadań Agencji płatniczej do podmiotów wdrażających – do wymagań normy ISO/IEC 27001, z uwzględnieniem niniejszych *Zaleceń*.

Zalecenia przekładają się na następujące zasady współpracy między Agencją płatniczą, a podmiotem wdrażającym:

1. Wytyczne zawarte w Zaleceniach nie zastępują normy: ISO/IEC 27001 stanowią jedynie uzupełnienie wymaganych do wdrożenia i stosowania w obszarze dotyczącym zadań delegowanych norm ISO/IEC 27001.
2. Przyjęty model współpracy zakłada, że podmioty wdrażające korzystają z dostępu do systemu teleinformatycznego udostępnionego przez Agencję płatniczą używając określonych formularzy internetowych (tj. poprzez przeglądarkę internetową).
3. Zawarte w Zaleceniach wytyczne powinny znaleźć odzwierciedlenie w wewnętrznych dokumentach podmiotów wdrażających i być wprowadzone w życie w sposób formalnie przyjęty przez te podmioty.
4. Wymagane jest, aby wdrożenie Zaleceń dotyczących bezpieczeństwa informacji w podmiotach wdrażających odbyło się zgodnie z Harmonogramem dojścia do osiągnięcia gotowości do wykonywania przez podmioty wdrażające zadań delegowanych przez Agencję płatniczą w ramach Planu Strategicznego dla Wspólnej Polityki Rolnej na lata 2023 - 2027 i znalazło odzwierciedlenie w Deklaracji gotowości lub Warunkowej deklaracji gotowości.

II. NADZÓR NAD BEZPIECZEŃSTWEM INFORMACJI

1. Kierownik podmiotu wdrażającego realizuje nadzór i kontrolę nad bezpieczeństwem informacji, bezpośrednio lub za pośrednictwem wyznaczonego pracownika pełniącego funkcję Inspektora Bezpieczeństwa Informacji (IBI).
2. Czynności kontrolne w ramach nadzoru nad bezpieczeństwem informacji realizowane są w terminach określonych harmonogramem realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowywanym na każdy rok kalendarzowy.
3. Harmonogram realizacji zadań kontrolnych, nadzorczych i szkoleniowych opracowuje Inspektor Bezpieczeństwa Informacji w uzgodnieniu z kierownikiem podmiotu wdrażającego lub osobiście kierownik podmiotu wdrażającego.
4. Wskazane jest prowadzenie następujących czynności kontrolnych:
   1) kontrola uprawnień dostępu użytkowników, tj. czy:
      - stosowane są unikalne identyfikatory zgodne z przyjętym schematem;
      - zablokowane zostały wszystkie zbędne identyfikatory (konta użytkowników);
      - przyznane uprawnienia dostępu do systemu teleinformatycznego są zgodne z wnioskiem o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą;
      - przyznane uprawnienia są zgodne z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy;
      - uprawnienia zawarte we wniosku o nadanie / zmianę uprawnień, określonym przez Agencję płatniczą, są zgodne z zakresem upoważnienia do przetwarzania danych osobowych lub innych informacji wrażliwych (jeżeli dotyczy);
      - terminy obowiązywania uprawnień są aktualne;
      - użytkownicy zostali poinformowani o zakresie swoich uprawnień i pisemnie potwierdzili zapoznanie się z nimi;
   2) kontrola wymagań bezpieczeństwa na stanowiskach realizujących zadania delegowane:
      - sprawdzenie, czy dostęp do systemu teleinformatycznego wynikający z realizacji zadań delegowanych jest zgodny z aktualnym zakresem obowiązków pracownika;
   3) kontrola ewidencji osób, którym nadano upoważnienia do przetwarzania danych osobowych, tj. czy:
      - prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych jest kompletna i poprawna;
      - osoby upoważnione zostały przeszkolone z zakresu ochrony danych osobowych i podpisały stosowne oświadczenie.
5. Z każdej kontroli powinien być sporządzony raport.

III. PODSTAWOWE WYMAGANIA I OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU TELEINFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ

A. Szkolenia dla użytkowników systemu teleinformatycznego

1. Warunkiem uzyskania dostępu przez pracownika do systemu teleinformatycznego powinno być odbycie szkolenia z zakresu bezpieczeństwa informacji przeprowadzone przez uprawnionego pracownika podmiotu wdrażającego. Szkolenia użytkowników systemu teleinformatycznego mają na celu uzyskanie przez nich optymalnego poziomu wiedzy i umiejętności, które pozwolą właściwie użytkować i chronić system teleinformatyczny.
2. Okresowo (nie rzadziej niż raz na rok) powinny być przeprowadzane szkolenia doskonalące z zakresu bezpieczeństwa informacji. Szkolenia powinny obejmować zagadnienia, które w szczególności dotyczą:
   1) zapoznania użytkowników z obowiązującymi regulacjami prawnymi dotyczącymi ochrony informacji;
   2) przygotowania użytkowników do właściwego korzystania z powierzonych zasobów (instrukcje użytkowania sprzętu i aplikacji, itp.);
   3) sposobu postępowania w przypadku zdarzenia (np. incydentu) związanego z naruszeniem bezpieczeństwa informacji;
   4) sposobów postępowania w sytuacjach awaryjnych i kryzysowych.

B. Używanie autoryzowanych środków do przetwarzania informacji

1. Każdy środek do przetwarzania informacji powinien podlegać inwentaryzacji i autoryzacji (dopuszczenie do pracy w systemie teleinformatycznym).
2. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
3. Użytkowników obowiązuje zakaz testowania lub podejmowania prób przełamywania zabezpieczeń systemu teleinformatycznego.

C. Wynoszenie mienia i korzystanie z urządzeń przenośnych

1. Przez urządzenia przenośne, które mogą służyć do przetwarzania i przechowywania informacji poza siedzibą rozumie się nie tylko wszelkie formy komputerów osobistych, ale także wszelkie rodzaje organizerów, telefonów przenośnych, kart procesorowych i innych rodzajów nośników elektronicznych, magnetycznych i optycznych, używanych do pracy poza biurem podmiotu wdrażającego. Dokumenty papierowe podlegają szczególnej ochronie polegającej na zabezpieczaniu ich przed osobami nieuprawnionymi ze szczególnym uwzględnieniem ich transportu. Dopuszczalna jest praca na dokumentach papierowych poza siedzibą, w wyjątkowych sytuacjach.
2. Dokumenty wydaje się osobom uprawnionym do pracy poza siedzibą za pokwitowaniem. Komputery przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera hasłem. Ich używanie poza strefą administracyjną musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.

3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów 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 biurem podmiotu wdrażającego, jeśli pozostają w postaci niezaszyfrowanej.
5. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza biurem podmiotu wdrażającego, obowiązany jest do wystąpienia do pracownika bądź komórki odpowiedzialnej za utrzymanie infrastruktury informatycznej z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia kryptograficzne oraz ochronę antywirusową.
6. W przypadku utraty powierzonego urządzenia przenośnego używanego poza biurem podmiotu wdrażającego użytkownik niezwłocznie powinien powiadomić o tym fakcie bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłosić ten fakt na policję, traktując jako incydent bezpieczeństwa. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

D. **Korzystanie z systemu teleinformatycznego udostępnionego przez Agencję płatniczą**

1. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
2. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika, na podstawie wniosku o nadanie / zmianę uprawnień, złożonego na wzorze i zgodnie z zasadami określonymi przez Agencję płatniczą.
3. Każdy użytkownik musi posiadać w systemie teleinformatycznym unikalny identyfikator.
4. Użytkownik ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
5. W przypadku 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 dostęp do systemu informatycznego.
6. Na stacjach roboczych, na których wykonywane są zadania delegowane, powinno być zabronione m.in.:

1) umożliwianie dostępu do systemu teleinformatycznego osobom nieupoważnionym;
2) rejestrowanie się w systemie teleinformatycznym na identyfikatorze innego użytkownika;
3) korzystanie z konta innego użytkownika;
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 systemu teleinformatycznego;
6) samowolnego modyfikowania ustawień związanych z bezpieczeństwem w systemie informatycznym;
7) świadome wprowadzanie błędnych danych do systemu informatycznego;
8) udostępnianie danych osobom nieupoważnionym;
9) przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne;
10) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania i danych;
11) korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

E. **Ochrona haseł i kluczy kryptograficznych**

1. Hasła użytkowników lub inne dane uwierzytelniające muszą podlegać szczególnej ochronie.
2. Każdy użytkownik systemu teleinformatycznego w podmiocie wdrażającym zobowiązany jest do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie teleinformatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) poinformowania Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   4) stosowania haseł o minimalnej długości 12 znaków, zawierających kombinację małych i dużych liter oraz cyfr i znaków specjalnych;
   5) zmiany wykorzystywanych haseł w regularnych odstępach czasu.
3. Zabronione powinno być:
   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).
4. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

5. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Inspektorowi Bezpieczeństwa Informacji lub kierownikowi podmiotu wdrażającego.

F. **Zasady „czystego biurka i czystego ekranu”**

1. Podmiot wdrażający powinien prowadzić „politykę czystego biurka i ekranu” obejmującą następujące zasady:
   1) wszelkie dokumenty papierowe i nośniki elektroniczne zawierające dane związane z wykonywaniem zadań delegowanych, kiedy nie są używane, powinny być przechowywane w zamkniętym urządzeniu meblowym (sejf, szafa lub inna forma zabezpieczenia) szczególnie, jeśli w pomieszczeniu biurowym czasowo nie ma pracownika wykonującego te zadania i odpowiadającego za bezpieczeństwo danych;
   2) monitory stacji roboczych należy ustawiać w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu;
   3) komputery osobiste i stacje robocze pozostawiane bez nadzoru lub czasowo nieużywane muszą być wyrejestrowane z sieci lub zablokowane (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub za pomocą innego podobnego mechanizmu);
   4) po zakończeniu pracy należy wylogować się z systemu i wyłączyć komputer; niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia systemu lub przez wyłączenie napięcia zasilającego;
   5) po zakończeniu pracy stanowisko pracy powinno być uporządkowane, w celu uniemożliwienia dostępu osób nieupoważnionych do dokumentów zawierających dane wrażliwe;
   6) punkty przyjmowania i wysyłania korespondencji papierowej winny być odpowiednio zabezpieczone;
   7) w miejscach, gdzie przetwarzane są dane dotyczące zadań delegowanych powinien być wprowadzony zakaz korzystania bez autoryzacji z fotokopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych itp.);
   8) wszelkie wydruki zawierające informacje związane z zadaniami delegowanymi powinny być niezwłocznie usuwane z drukarek, a wydruki uszkodzone natychmiast niszczone w niszczarce dokumentów;
   9) nie należy pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach;
   10) należy przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi lub okien podczas nieobecności w pomieszczeniu.

G. **Zgłaszanie zdarzeń o naruszeniu bezpieczeństwa informacji**

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 m.in.:
   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) pojawianie się nietypowych komunikatów na ekranie;
   7) niemożność zalogowania się do systemu teleinformatycznego;
   8) spowolnienie pracy oprogramowania;
   9) niestabilna praca systemu teleinformatycznego;
   10) brak reakcji systemu na działania użytkownika;
   11) ponowny start lub zawieszanie się komputera;
   12) ograniczenie funkcjonalności oprogramowania.
3. Wszelkie działania użytkownika związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.
4. Dokonywanie zmian w miejscu naruszenia ochrony bez wiedzy i zgody Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.
5. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędach 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 Inspektora Bezpieczeństwa Informacji lub kierownika podmiotu wdrażającego oraz swojego bezpośredniego przełożonego.

IV. BEZPIECZEŃSTWO FIZYCZNE

1. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego powinien wynikać z przeprowadzonego i udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
   1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.);
   2) określenie kategorii potencjalnych zagrożeń obiektu (wewnętrznych i zewnętrznych) w szczególności pożaru, powodzi, katastrof środowiskowych;
   3) opisu topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące) w szczególności bliskość terenów przemysłowych;
   4) odnotowanych w przeszłości czynów przestępczych (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa);
   5) aktualnego stanu bezpieczeństwa obiektu;
   6) opisu i oceny funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualnego stanu technicznego (poziom technologiczny, sprawność, dokumentacja, serwisowanie);
   7) aktualnego stanu ochrony fizycznej obiektu;
   8) opisu stosowanych procedur i rozwiązań organizacyjnych;
   9) wniosków, co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno–organizacyjnych);
   10) propozycji doskonalenia systemów oraz procedur ochrony obiektu.
3. Za opracowanie oraz stałą aktualizację planu ochrony fizycznej uwzględniającego wyniki szacowania ryzyka winien odpowiadać kierownik podmiotu wdrażającego lub pracownik, któremu powierzono zakres obowiązków związanych z zapewnieniem bezpieczeństwa fizycznego.

A. Obszary bezpieczne

1. Każdy podmiot wdrażający powinien wydzielić z obszaru zajmowanego przez komórki organizacyjne strefę administracyjną i strefę ogólnodostępną. Stacje robocze obsługujące zadania delegowane powinny być zlokalizowane w strefie administracyjnej.
2. Ochrona strefy administracyjnej oraz zastosowane środki bezpieczeństwa powinny być zgodne z zasadami określonymi w ustawie o ochronie osób i mienia i wynikać z opracowanego Planu Ochrony podmiotu wdrażającego.
3. W uzasadnionych przypadkach, gdy czynności związane z realizacją zadań delegowanych muszą być wykonywane przez podmiot wdrażający w ogólnodostępnej strefie, należy dodatkowo przyjąć następujące zasady:

1) strefa administracyjna dla zadań delegowanych może zostać zawężona do miejsc przechowywania bieżącej dokumentacji dotyczącej tych zadań, np. do zamykanych szaf biurowych;
2) stanowiska komputerowe, na których przetwarzane są informacje dotyczące zadań delegowanych powinny:
   - być tak usytuowane, aby uniemożliwić nieuprawnionym osobom przebywającym w pomieszczeniu podgląd danych wyświetlanych na monitorze lub wyprowadzanych na drukarkę;
   - stanowisko powinno być fizycznie wydzielone od pozostałej części pomieszczenia (np. barierką, słupkami i taśmą oddzielającą, itp.);
3) pracownicy w trakcie wykonywania zadań delegowanych odpowiadają bezpośrednio za zabezpieczenie stanowiska komputerowego oraz miejsc przechowywania dokumentacji przed fizycznym dostępem osób trzecich, w tym także przed możliwością podglądu informacji wyświetlanych na ekranie monitora lub drukowanych na drukarce;
4) w przypadku czasowej nieobecności pracownika wykonującego zadania delegowane, stanowisko komputerowe oraz miejsca przechowywania dokumentacji muszą być skutecznie zabezpieczone przed dostępem lub podglądem osób nieupoważnionych;

4. Wykonywanie w ogólnodostępnej strefie zadań delegowanych przez podmiot wdrażający musi być poprzedzone szacowaniem ryzyka i jest dopuszczalne wtedy, gdy poziom ryzyka nie przekracza akceptowalnego poziomu ryzyka.

B. **Zarządzanie kluczami**

1. Klucze wydawać należy na podstawie rejestru osób upoważnionych do ich pobierania, po sprawdzeniu tożsamości osoby pobierającej klucz. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowywany.
2. Za organizację wydawania kluczy do pomieszczeń, w tym za przyznanie i odebranie prawa do ich pobierania, odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
3. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada kierownik podmiotu wdrażającego lub osoba przez niego wyznaczona.
4. Pozostawanie osób po godzinach służbowych w pracy wymaga, aby spełnione były następujące warunki:
   1) każdy pracownik pozostający po godzinach służbowych w pracy musi mieć wyrażoną zgodę na pozostanie przez kierownika komórki organizacyjnej;
   2) jeśli po godzinach służbowych pozostaje więcej niż jedna osoba, kierownik komórki organizacyjnej (lub urzędu) wyznacza z tej grupy osobę, która będzie odpowiedzialna za właściwe zabezpieczenie obiektu (m.in. uzbrojenie instalacji alarmowej, zamknięcie drzwi wejściowych bądź dopilnowanie tych czynności w przypadku, gdy ktoś inny to wykonuje);

3) jeśli w danym dniu pozostają pracownicy po godzinach służbowych, to obowiązkiem osoby upoważnionej do zabezpieczenia i zamknięcia obiektu po zakończonej pracy, jest pobranie kluczy – na podstawie uzyskanej zgody na pozostanie w pracy.

C. **Lokalizacja oraz ochrona sprzętu i dokumentacji**

1. Środki przetwarzania informacji dotyczącej zadań delegowanych muszą spełniać następujące wymagania bezpieczeństwa:
   1) lokalizacja sprzętu powinna zapewnić minimalizację niepotrzebnego dostępu do obszarów pracy;
   2) lokalizacja środków przetwarzania powinna minimalizować ryzyko podejrzenia przez nieuprawnione osoby, a lokalizacja urządzeń przechowujących informacje zabezpieczać przed nieautoryzowanym dostępem.
2. Pomieszczenia, w których znajdują się szafy do przechowywania dokumentacji dotyczącej zadań delegowanych, powinny posiadać system sygnalizacji pożaru oraz system sygnalizacji włamania.
3. Urządzenia infrastruktury zabezpieczającej muszą być przeglądane i konserwowane zgodnie z instrukcjami i wymaganiami ich producentów.

V. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU ZASOBAMI LUDZKIMI

1. Warunki przystąpienia do pracy, w zależności od zakresu obowiązków, powinny uwzględniać następujące aspekty bezpieczeństwa:
   1) przeszkolenie pracownika w zakresie tematycznym wynikającym z obowiązków i odpowiedzialności na zajmowanym stanowisku;
   2) oświadczenie pracownika o zapoznaniu się z odpowiednimi regulaminami, procedurami i przepisami w sprawie bezpieczeństwa informacji;
   3) przeszkolenie pracownika z zakresu bezpieczeństwa informacji (w tym ochrony danych osobowych), które przeprowadzić należy przed uzyskaniem dostępu do zasobów informacyjnych Agencji płatniczej;
   4) zobowiązanie pracownika do zachowania w poufności informacji wrażliwych, również poza biurem podmiotu wdrażającego i godzinami pracy, a także po ustaniu zatrudnienia bądź zakończeniu wykonywania usług na rzecz podmiotu wdrażającego;
   5) nadanie upoważnienia pracownikowi do przetwarzania danych osobowych.

VI. ZASADY EKSPLOATACJI SYSTEMU TELEINFORMATYCZNEGO UDOSTĘPNIONEGO PRZEZ AGENCJĘ PŁATNICZĄ

A. Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery podmiotu wdrażającego powinny być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym.
2. Użytkowane poza systemem podmiotu wdrażającego wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemie teleinformatycznym, należy sprawdzić za pomocą aktualnego oprogramowania antywirusowego.

B. Zasady bezpieczeństwa sieci

1. Sieć informatyczna podmiotu wdrażającego powinna być podłączona do sieci ogólnodostępnych (w szczególności sieci publicznej Internet) przy użyciu specjalnych systemów zabezpieczających, np. aplikacji i urządzeń typu firewall, systemów IDS (Intrusion Detection System) i IPS (Intrusion Prevention System).
2. Reguły filtrowania zapór sieciowych powinny być ustalane i regularnie weryfikowane w zależności od pojawiających się zagrożeń.
3. Wymagania odnoszące się do elementów bezpieczeństwa, poziomu usług i zarządzania wszystkimi usługami sieci muszą być jednoznacznie określone i włączone do odpowiednich umów na dostarczanie tych usług, niezależnie od tego, czy są one częściowo realizowane własnymi środkami, czy zlecane w całości na zewnątrz.

C. Identyfikacja i uwierzytelnianie użytkowników

1. Prawa dostępu do systemu teleinformatycznego przydziela poszczególnym pracownikom podmiotu wdrażającego pracownik pełniący rolę lokalnego administratora podmiotu wdrażającego. Rolę tę nadaje administrator systemu teleinformatycznego Agencji płatniczej. Dostęp do funkcji administracyjnych systemu z poziomu podmiotu wdrażającego jest możliwy tylko dla użytkownika w roli lokalnego administratora podmiotu wdrażającego.
2. Lokalny administrator podmiotu wdrażającego prowadzi rejestr użytkowników z nadanymi uprawnieniami.
3. Do obowiązków lokalnego administratora podmiotu wdrażającego należy także sprawdzanie i blokowanie zbędnych identyfikatorów użytkowników oraz ich kont, aby nie mogły być one wykorzystane powtórnie przez innych użytkowników.
4. Lokalny administrator podmiotu wdrażającego poprzez ustawienia systemowe wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane. Hasło tymczasowe, dostarczane w przypadku, gdy użytkownik zapomni hasła, może być wydane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej.

6. Kontrola praw dostępu użytkowników realizowana jest przez lokalnego administratora podmiotu wdrażającego według następujących zasad:
   1) prawa dostępu użytkowników są przeglądane w regularnych odstępach czasu (nie rzadziej niż co sześć miesięcy) oraz każdorazowo po wprowadzeniu zmian w tych prawach;
   2) w przypadku zmiany miejsca zatrudnienia pracownika, dokonuje się dodatkowego przeglądu i ponownego nadania praw dostępu;
   3) przydzielone uprawnienia są kontrolowane w regularnych odstępach czasu w celu sprawdzenia, czy nie przyznano nadmiarowych uprawnień;
   4) uprawnienia do korzystania ze specjalnie uprzywilejowanych praw dostępu (np. prawa administratora) winny być przeglądane nie rzadziej niż co trzy miesiące;
   5) powinna być prowadzona rejestracja zmian uprzywilejowanych kont na potrzeby okresowych przeglądów;
   6) każde dokonanie kontroli praw dostępu użytkowników powinno zostać udokumentowane sporządzeniem raportu, który należy załączyć do prowadzonej dokumentacji przez lokalnego administratora podmiotu wdrażającego.

D. Zarządzanie wymiennymi nośnikami danych

1. Wymienne nośniki informacji (taśmy, pamięci typu flash, wyjmowane dyski twarde, płyty CD i DVD oraz wydruki) zawierające informacje wrażliwe należy przechowywać w miejscach uniemożliwiających dostęp do nich osobom nieuprawnionym.
2. Wszystkie nośniki informacji muszą być przechowywane w bezpiecznym środowisku w warunkach zgodnych z wymaganiami producenta. W przypadku, gdy czas życia nośnika (określony przez producenta) jest krótszy od sumarycznego czasu przechowywania informacji, należy dodatkowo zapewnić, aby na skutek pogorszenia się jakości nośnika nie nastąpiła utrata informacji.
3. Magnetyczne nośniki informacji zawierające kopie bezpieczeństwa oraz informacje archiwalne należy przechowywać w specjalnych, atestowanych, metalowych szafach do przechowywania magnetycznych nośników informacji. Pozostałe nośniki przechowywać i zabezpieczać należy zgodnie z wymaganiami obowiązującymi dla informacji na nich zapisanych.
4. Ograniczać należy do niezbędnego minimum liczby wytwarzanych kopii i wydruków.
5. Zbędne wydruki, notatki, kopie dokumentów, itp. – jeśli zawierają informacje wrażliwe – muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.
6. Wszystkie nośniki informacji (taśmy magnetyczne, płyty CD-ROM, wymienne dyski twarde, wydruki komputerowe i inne) wytworzone w systemach informatycznych i zawierające informacje wrażliwe, muszą być ewidencjonowane i oznakowane.
7. Etykiety nośników informacji powinny posiadać identyfikator lub numer umożliwiający ich jednoznaczną klasyfikację i znajdujący odzwierciedlenie w dzienniku ewidencji nośników.

8. Na podstawie etykiety nośnika informacji i danych zawartych w dzienniku ewidencji nośników powinno być możliwe ustalenie:
   1) numeru ewidencyjnego nośnika,
   2) typu nośnika,
   3) daty zapisu na nośniku,
   4) nazwy komórki organizacyjnej składującej informacje,
   5) określenia rodzaju przechowywanej informacji,
   6) imienia i nazwiska osoby dokonującej zapisu.
9. Wycofane nośniki informacji, które były wykorzystywane do przetwarzania informacji wrażliwych, nie mogą być wynoszone poza teren jednostki wdrażającej, w której były użytkowane, bez wcześniejszego skutecznego usunięcia danych.
10. Uszkodzone nośniki, takie jak dyski twarde, i i taśmy magnetyczne, płyty CD-ROM i inne komputerowe nośniki danych, zawierające informacje wrażliwe, należy komisyjnie niszczyć w sposób uniemożliwiający odczytanie zapisanych na nich informacji (np. zgniatanie, łamanie, działanie silnym polem magnetycznym).
11. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia powinno być poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.

E. Konserwacja i naprawa sprzętu

1. Sprzęt informatyczny winien podlegać konserwacji według ustalonego planu, wynikającego z zaleceń jego producenta.
2. Konserwacja i naprawy mogą być prowadzone jedynie przez uprawniony personel lub podmiot zewnętrzny świadczący tego rodzaju usługi na podstawie umowy lub w ramach gwarancji.
3. W przypadku, gdy na nośnikach informacji, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje wrażliwe, sprzęt taki naprawiany powinien być pod nadzorem uprawnionego pracownika podmiotu wykonującego zadania delegowane. Jeżeli taki nadzór nie jest możliwy, informacja wrażliwa musi zostać skutecznie usunięta. O ile zachodzi taka możliwość, usuwana informacja powinna być uprzednio zarchiwizowana.
4. Jeżeli gwarant, w ramach naprawy gwarancyjnej, żąda zwrotu urządzenia służącego do przechowywania informacji, informacja wrażliwa znajdująca się w takim urządzeniu musi zostać z niego trwale usunięta. Sposób usuwania danych z nośnika powinny określać szczegółowe procedury.
5. Umowy zawierające gwarancję dostawcy lub producenta muszą zawierać sformułowania umożliwiające realizację postanowień ust. 4 bez utraty gwarancji.
6. W przypadku zbywania sprzętu, bądź przekazywania go do ponownego użycia, należy skutecznie usunąć z niego informacje wrażliwe. Sposób usuwania danych muszą określać szczegółowe procedury.

F. Zarządzanie dostępem do systemu operacyjnego

1. Wszystkie konta użytkowników na stacjach roboczych, na których wykonywane są zadania delegowane, powinny być skonfigurowane z uprawnieniami systemowymi „użytkownik”.
2. Użytkownik systemu operacyjnego powinien być jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
4. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
5. Uprawnienia dostępu mogą być nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) powinno być traktowane jako incydent związany z bezpieczeństwem informacji.

VII. OCHRONA DANYCH OSOBOWYCH

1. Kierownik podmiotu wdrażającego wykonuje obowiązki Administratora danych wobec powierzonych mu danych.
2. Kierownik podmiotu wdrażającego odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności, w odniesieniu do wykonywania zadań delegowanych, odpowiada za:
   1) zgodne z prawem (w szczególności z ustawą o ochronie danych osobowych) przetwarzanie danych osobowych;
   2) zapewnienie, aby zgromadzone dane osobowe były merytorycznie poprawne, a ich zakres i rodzaj był adekwatny do celów, w jakich są przetwarzane;
   3) nadawanie upoważnień do przetwarzania danych osobowych;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w, ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
   5) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
3. Upoważnienie do przetwarzania danych osobowych nadaje się przed dopuszczeniem osoby do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych. Upoważnienie odbiera się niezwłocznie po ustaniu celu, dla którego zostało nadane.
4. Upoważnienie do przetwarzania danych osobowych nadawane jest pracownikom, bez względu na podstawę prawną zatrudnienia, po odbyciu szkolenia z ochrony danych osobowych, a fakt odbycia przeszkolenia pracownik powinien potwierdzić podpisując stosowne oświadczenie.

VIII. BEZPIECZEŃSTWO INFORMACJI W ZARZĄDZANIU CIĄGŁOŚCIĄ DZIAŁANIA

1. W przypadku, gdy podmiot wdrażający nie posiada planu PZCD, niezbędne jest opracowanie dokumentu, który określi warunki realizacji zadań delegowanych w sytuacji wystąpienia kryzysu. Dokument taki powinien uwzględniać następujące czynniki:
   1) rozpoznanie i uzgodnienie wszystkich procedur awaryjnych i zakresów odpowiedzialności w obszarze zadań delegowanych;
   2) wdrożenie procedur awaryjnych tak, aby umożliwić naprawę i przywrócenie działania w wymaganym czasie z uwzględnieniem zewnętrznych zależności biznesowych (pomiędzy podmiotem wdrażającym a Agencją płatniczą) oraz realizowanych procesów;
   3) dokumentację uzgodnionych procedur oraz procesów operacyjnych i pomocniczych;
   4) przeszkolenie personelu w zakresie uzgodnionych procedur awaryjnych, w tym w zakresie zarządzania w sytuacjach kryzysowych;
   5) procedury awaryjne objęte powyższym dokumentem powinny być przetestowane w roku, w którym uruchomiono realizację zadań delegowanych, a następnie w cyklu rocznym testy winny być powtarzane.
2. Jeśli podmiot wykonujący zadania delegowane opracował i utrzymuje aktualny plan działania PZCD, to do powyższego planu należy włączyć procedury określające sposób postępowania z zadaniami delegowanymi na wypadek wystąpienia kryzysu.

Zasady przepływu informacji dotyczące szczegółowych warunków i trybu przyznawania i zatwierdzania pomocy finansowej oraz stosowania procedur w zakresie zadań delegowanych przez Agencję płatniczą do podmiotów wdrażających w ramach PS WPR na lata 2023 -2027

Słownik

AP	Agencja płatnicza – Agencja Restrukturyzacji i Modernizacji Rolnictwa (ARiMR)
DAiK	Departament Audytu i Kontroli ARiMR
DDD	Departament Działań Delegowanych ARiMR
DBRiKT	Departament Baz Referencyjnych i Kontroli Terenowych ARiMR
DAiS	Departament Analiz i Sprawozdawczości ARiMR
DZN	Departament Zarządzania Należnościami ARiMR
DK	Departament Księgowości ARiMR
DF	Departament Finansowy ARiMR
DPiZP	Departament Prawny i Zamówień Publicznych ARiMR
IZ	Instytucja Zarządzająca – Minister Rolnictwa i Rozwoju Wsi
Departament WPR	Departament Wspólnej Polityki Rolnej w Ministerstwie Rolnictwa i Rozwoju Wsi
PW	Podmiot wdrażający, o którym mowa w art. 2 pkt 22 ustawy z dnia 8 lutego 2023 r. o Planie Strategicznym dla Wspólnej Polityki Rolnej na lata 2023-2027
KP	Książka Procedur
KPH	Książka Procedur Horyzontalna
PS WPR na lata 2023-2027	Plan Strategiczny dla Wspólnej Polityki Rolnej na lata 2023-2027
PUE	Platforma Usług Elektronicznych
System IT	System teleinformatyczny ARiMR, o którym mowa w art. 10 c ustawy o ARiMR z dnia 9 maja 2008 r.
CSOB	Centralny System Obsługi Beneficjenta, który stanowi podstawowe narzędzie obsługi interwencji Planu Strategicznego na lata 2023-2027,

I. Cel

Celem dokumentu jest przyjęcie jednolitych zasad przepływu informacji dotyczących szczegółowych warunków i trybu przyznawania i zatwierdzania pomocy finansowej oraz stosowania procedur w zakresie zadań delegowanych przez AP do PW w ramach PS WPR na lata 2023-2027.

Z uwagi na liczbę podmiotów zaangażowanych w realizację zadań delegowanych istotne jest zapewnienie właściwego i skutecznego systemu komunikacji pomiędzy podmiotami. Pozwoli to uniknąć wydawania wzajemnie wykluczających się stanowisk, nieterminowego przekazywania informacji, nieotrzymania informacji przez wszystkich wymaganych adresatów lub otrzymania ich zbyt późno.

Przygotowanie formalnych zasad komunikacji związane jest w szczególności z koniecznością wypełnienia wymogu akredytacyjnego określonego w załączniku I do rozporządzenia delegowanego Komisji (UE) 2022/127 z dnia 7 grudnia 2021 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/2116 o przepisy dotyczące agencji płatniczych i innych organów, zarządzania finansami, rozliczania rachunków, zabezpieczeń oraz stosowania euro (Dz. Urz. UE L 20 z 31.01.2022, str. 95 z późn. zm.).

Zobowiązanie do stosowania zasad przepływu informacji wynika z postanowień umowy delegowania zadań AP do PW.

II. Zasady ogólne

1. AP jest podmiotem odpowiedzialnym za koordynację przepływu informacji w obszarze zadań delegowanych przez AP, w szczególności za gromadzenie, udostępnianie i przekazywanie informacji w zakresie:
   - szczegółowych warunków i trybu przyznawania oraz zatwierdzania pomocy finansowej,
   - stosowania procedur dotyczących zadań delegowanych przez AP,
   - zmian w zakresie stosowania procedur i instrukcji dotyczących zadań delegowanych przez AP,
   - obsługi systemu IT.

2. Korespondencja pomiędzy AP i PW odbywa się każdorazowo w formie korespondencji elektronicznej lub za pośrednictwem elektronicznej skrzynki podawczej ePUAP.

   W celu usprawnienia przepływu informacji pomiędzy AP i PW możliwe jest wysłanie skanu pisma za pośrednictwem poczty elektronicznej, (zgodnie z listą mailingową).

   Nie ma konieczności wysyłania korespondencji w wersji papierowej, o ile przepisy nie stanowią inaczej.

   Lista mailingowa zostanie utworzona w celu określenia osób odpowiedzialnych za przepływ informacji pomiędzy AP i PW oraz zamieszczona w Chmurze ARiMR.

   Informacja dotycząca adresów poczty elektronicznej wyznaczonych w PW osób – PW przekazują w wersji elektronicznej na adres poczty elektronicznej: delegowane@arimr.gov.pl oraz zamieszczają w Chmurze ARiMR, we wskazanym przez AP katalogu.

   W sytuacji wystąpienia konieczności aktualizacji adresów:

   – PW wysyła informację o aktualizacji na adres poczty elektronicznej: delegowane@arimr.gov.pl, za pośrednictwem poczty elektronicznej i zamieszcza w Chmurze ARiMR, we wskazanym przez AP katalogu.

   – AP wysyła informację o aktualizacji, za pośrednictwem poczty elektronicznej na adresy PW (zgodnie z listą mailingową przekazaną przez PW) i zamieszcza w Chmurze ARiMR, we wskazanym katalogu zaktualizowaną listę mailingową.

   Pisma kierowane do AP powinny być przekazywane w wersji elektronicznej (skan dokumentów) na adres poczty elektronicznej wyznaczonych osób w AP (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027) oraz do wiadomości delegowane@arimr.gov.pl.

   Pismo:

   a. PW zawierające:

   - pytanie w odniesieniu do zadań delegowanych / zagadnień merytorycznych,
   - przekazanie tabeli uwag do dokumentów,

   powinno być podpisane przez upoważnioną osobę w PW (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027).

   b. AP zawierające

   - pytanie / odpowiedź na pytanie PW w odniesieniu do zadań delegowanych / zagadnień merytorycznych,
   - przekazanie dokumentów do opiniowania,

   powinno być podpisane przez upoważnioną osobę w AP (np. Dyrektor / Zastępca Dyrektora komórki odpowiedzialnej za zakres merytoryczny w ramach PS WPR na lata 2023-2027).

   Wyjątkiem jest przekazanie KP/KPH do stosowania.

Po uprzednim zatwierdzeniu KP / KPH w AP do PW zostanie przekazana informacja o zatwierdzeniu KP / KPH i obowiązującym terminie przyjęcia jej do stosowania, w postaci papierowej, podpisanej przez Zastępcę Prezesa AP (lub osobę upoważnioną).

Ww. informacja przekazywana jest również na adresy poczty elektronicznej Dyrektorów PW i Departamentu WPR oraz osób wyznaczonych w PW i Departamencie WPR zgodnie z listą mailingową.

3. Jeżeli przygotowanie przez AP stanowiska wymaga interpretacji kwestii generalnych wynikających z przepisów prawa powszechnie obowiązującego, AP występuje do IZ, zgodnie z zasadami występowania przez kierownictwo jednostek nadzorowanych do ministerstwa o interpretację w danym zakresie.

   Podstawę systemu realizacji PS WPR na lata 2023-2027 stanowią jego postanowienia, przepisy prawa powszechnie obowiązującego, Wytyczne IZ oraz regulaminy naborów wniosków.

4. Niniejsze zasady nie obowiązują w sprawach związanych z trybem składania wniosku o przeprowadzenie kontroli doraźnej przez Prezesa Urzędu Zamówień Publicznych.

III. Zasady szczegółowe

1. Przekazywanie pytań

1) Kierowane do AP pytania muszą zawierać:
   a) opis - problemu, zagadnienia, stanu faktycznego,
   b) opinię służb prawnych (jeśli pytanie związane jest z interpretacją przepisów prawa powszechnie obowiązującego),
   c) stanowisko PW w sprawie.

2) PW przekazują wszystkie pytania do AP. Departamentem wiodącym w obszarze zadań delegowanych przez AP jest DDD ARiMR.

3) Jeżeli pytania dotyczą kwestii będących w kompetencjach DBRiKT, DAiK, DZN, DAiS, DK lub DF należy je kierować zgodnie z właściwością:

   – kontrola (kontrola w rozumieniu art. 100 ust. 1 ustawy) oraz stosowanie procedur w tym zakresie – DBRiKT,

   – audyty i ich ustalenia – DAiK,

   – zlecenia zgłoszenia należności (ZW-1 i inne dokumenty towarzyszące) – DZN,

   – monitorowanie i sprawozdawczość oraz stosowanie procedur w tym zakresie – DAiS,

   – dokumenty finansowo-księgowe (zlecenie płatności , korekta zlecenia płatności lub noty) – DK lub DF.

   Pytania należy przesyłać na adresy wyznaczonych osób w AP (zgodnie z kompetencją) oraz do wiadomości DDD, zgodnie z zasadami określonymi w sekcji II pkt. 2.

   Informacja z adresami poczty elektronicznej wyznaczonych osób w AP zostanie przekazana do sekretariatu PW oraz zamieszona w Chmurze ARiMR, we wskazanym przez AP katalogu.

2. Udzielanie odpowiedzi

1) Przygotowanie odpowiedzi AP (DDD).

   Odpowiedzi na pytania przygotowywane są w terminie 30 dni kalendarzowych od wpływu do AP pytania z zastrzeżeniem przypadków, w których odpowiedź zostanie udzielona niezwłocznie po uzgodnieniu stanowiska.

   Jeśli pytania dotyczą również kwestii będących w kompetencjach innych komórek AP lub wymagają konsultacji z innymi komórkami AP, DDD występuje do odpowiedniej komórki o

opinię / stanowisko. Czas na udzielenie odpowiedzi przez DDD w tym przypadku wydłuży się o czas niezbędny na uzyskanie stanowiska z innej komórki ARiMR.

W przypadku, gdy pytanie PW wymaga od AP uzyskania interpretacji kwestii generalnych wynikających z postanowień PS WPR na lata 2023 – 2027, przepisów prawa powszechnie obowiązującego, Wytycznych IZ lub regulaminu naboru wniosków, AP występuje do IZ zgodnie z zasadami występowania przez kierownictwo jednostek nadzorowanych do ministerstwa o interpretację przepisów prawnych.

Ścieżka przekazania pytań do IZ dostosowana jest do obowiązujących zasad przekazywania dokumentów. Pytanie przekazywane jest również w formie skanu dokumentu na adresy elektroniczne Sekretariatu Departamentu WPR oraz osób wyznaczonych w Departamencie WPR.

W przypadku, gdy odpowiedź AP na pytanie PW wymaga od AP uzyskania stanowiska podmiotu zewnętrznego (innego niż IZ), DDD występuje do tego podmiotu o interpretację.

Odpowiedzi w określonej sprawie są przekazywane do PW, który skierował pytanie oraz do wiadomości pozostałych PW, jeśli mogą mieć zastosowanie w sprawach, które dotyczą podobnych zagadnień.

Wydawane stanowiska nie są rozstrzygnięciami AP w indywidualnych sprawach, a jedynie wyjaśnieniem generalnych zasad i mogą być pomocne w ocenie tych spraw.

2) Przygotowanie odpowiedzi AP (komórki inne niż DDD ARiMR).

Opisane w ppkt. 1 zasady dotyczą również odpowiedzi udzielanych przez DBRiKT, DAIK, DZN, DAiS, DK i DF.

Odpowiedzi na pytania przygotowywane przez departamenty inne niż DDD ARiMR są przekazywane do wiadomości DDD ARiMR.

3. Zatwierdzenie lub zmiana formularzy dokumentów aplikacyjnych (wniosków o przyznanie pomocy / wniosków o płatność), umów o przyznaniu pomocy oraz regulaminów naborów (jeśli dotyczy).

AP, przed zatwierdzeniem formularzy, przeprowadzi proces ich uzgodnienia z PW.

W tym celu AP udostępni PW w postaci makiet dokumentów powstałych w systemie IT, formularze dokumentów aplikacyjnych, umów o przyznaniu pomocy oraz regulaminów (jeśli dotyczy), a w sytuacji zaistnienia konieczności zmiany – przygotowuje aktualizację dokumentów.

Formularz umowy o przyznaniu pomocy oraz regulaminu naborów będą udostępniane przez AP jako pliki Word.

Następnie na adresy elektroniczne Dyrektorów PW oraz osób wyznaczonych w PW (zgodnie z listą mailingową) zostanie przekazana przez AP (DDD) informacja o rozpoczęciu konsultacji w zakresie nowych / zmienionych formularzy dokumentów, wraz z podaniem przyczyn zastosowanych zmian.

PW po dokonaniu analizy nowych / zmienionych formularzy przekazuje w terminie wskazanym przez AP, uwagi zgodnie ze wzorem Tabeli uwag zgłaszanych do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naborów /KP/KPH w ramach Interwencji ….. objętego PS WPR na lata 2023 -2027 (wzór tabeli stanowi załącznik nr 1 do niniejszych *Zasad (…)*).

Termin, wskazany w e-mailu AP, może zostać wydłużony na prośbę PW, w zależności od okoliczności w jakich dokonywane jest wprowadzenie lub zmiana formularzy. Informacja o wydłużeniu terminu zostanie przekazana przez AP do wszystkich PW.

Odpowiedź PW na prośbę AP podpisana przez upoważnioną osobę w PW (np. Dyrektor, Zastępca Dyrektora, Kierownik, Naczelnik komórki odpowiedzialnej za realizację PS WPR na lata 2023-2027) przekazywana jest w wersji elektronicznej do Dyrektora DDD i do wiadomości

wyznaczonych osób w AP oraz dodatkowo na adres poczty elektronicznej: delegowane@arimr.gov.pl.

Za przygotowanie zbiorczej *Tabeli zgłaszania uwag do formularza (…)* oraz nadanie statusów uwagom odpowiada AP (DDD). Zbiorcza tabela zostanie przekazana przez AP (DDD) bezzwłocznie do wszystkich PW.

W przypadku uwag o statusie nieuwzględniona lub uwzględniona w części zostanie wskazane przez AP (DDD) uzasadnienie braku możliwości jej uwzględnienia w całości, w części do PW.

Następnie AP(DDD) przeprowadza proces uzgadniania formularzy wewnątrz AP.

AP przekazuje do PW informację o nowym lub zmienionym formularzu oraz obowiązującym terminie jego stosowania (który nie może być wcześniejszy niż data przekazania) na elektroniczną skrzynkę podawczą ePUAP, podpisaną przez Zastępcę Prezesa AP (lub osobę upoważnioną).

Ww. informacja przekazywana jest również na adresy poczty elektronicznej Dyrektorów PW i Departamentu WPR oraz osób wyznaczonych w PW,(zgodnie z listą mailingową) i Departamencie WPR .

Zgłoszenie przez PW do AP (DDD) wad w funkcjonalności formularzy zaimplementowanych w systemie IT możliwe jest każdorazowo, gdy zostaną przez PW wykryte uchybienia.

4. Zatwierdzenie lub zmiana KP / KPH związanych z realizacją zadań delegowanych

AP opracowuje KP / KPH, a w sytuacji zaistnienia konieczności zmiany – wprowadza zmiany do KP / KPH i przygotowuje Kartę aktualizacji a następnie przekazuje do PW informację o rozpoczęciu konsultacji w zakresie nowej / zmienionej KP / KPH. Konsultacje te są prowadzone przed przekazaniem KP / KPH do opiniowania w AP.

Z uwagi na objętość KP / KPH AP zamieści dokumenty do konsultacji jedynie w Chmurze ARiMR (katalog zostanie wskazany w e-mailu z informacją o rozpoczęciu procesu konsultacji).

PW przekazują uwagi do AP, zgodnie ze wzorem *Tabeli zgłaszania uwag zgłaszanych do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naborów / KP/KPH w ramach Interwencji ….. objętego PS WPR na lata 2023 -2027* (wzór tabeli stanowi załącznik nr 1 do niniejszych *Zasad (…)*).

Po dokonanej analizie uwag zgłoszonych przez PW, w tym określeniu statusów do uwag, AP przekaże do PW:

a) wykaz uwag do KP / KPH, który stanowi załącznik nr 2 do niniejszych *Zasad (…)* – w przypadku nowej KP / KPH,
b) kartę aktualizacji do KP / KPH, która stanowi załącznik nr 3 do niniejszych *Zasad (…)* – w przypadku zmiany KP / KPH.

Za przygotowanie zbiorczego zestawienia uwag oraz nadanie statusów odpowiada AP, zgodnie z kompetencjami komórek merytorycznych AP.

Następnie przeprowadzany jest proces zatwierdzania KP / KPH w AP.

Po zatwierdzeniu KP / KPH w AP do PW zostanie przekazana informacja o zatwierdzeniu KP / KPH i obowiązującym terminie przyjęcia jej do stosowania.

Wyznaczony przez AP termin przyjęcia do stosowania KP / KPH nie powinien być krótszy niż 1 miesiąc od dnia przekazania KP / KPH. Możliwe jest skrócenie ww. terminu, po uprzednim uzgodnieniu odpowiednio: ze wszystkimi PW.

Uzgodnienie krótszego niż miesiąc terminu przyjęcia do stosowania KP / KPH, odbywa się poprzez przekazanie przez Dyrektora właściwej komórki AP, na adresy elektroniczne Dyrektorów PW oraz osób wyznaczonych w PW, propozycji AP w tym zakresie oraz otrzymanie informacji zwrotnej od Dyrektorów PW lub upoważnionych osób w PW, również w postaci elektronicznej w terminie 2 dni roboczych od przekazania przez AP propozycji.

Załącznik nr 1

Tabela zgłaszanych uwag do formularza dokumentu aplikacyjnego / umowy o przyznaniu pomocy / regulaminu naboru / KP / KPH [1] w ramach interwencji …….. objętego PS WPR na lata 2023 - 2027

Uwagi do treści zarządzenia					
Uwagi do formularza wniosku o przyznanie pomocy i załączników / instrukcji wypełniania wniosku o przyznanie pomocy / wniosku o płatność i załączników / instrukcji wypełniania wniosku o płatność / umowy o przyznaniu pomocy					
Lp.	Pozycja	Treść dotychczasowa	Uwagi / propozycje zapisu oraz Uzasadnienie	Zgłaszający uwagę	Status

[1] niepotrzebne usunąć

.

Załącznik nr 2

WYKAZ UWAG DO KP / KPH – właściwy symbol klasyfikacyjny RWA-…-ARiMR/…/

Znak sprawy:……..

Lp.	Treść uwagi	Nazwa komórki organizacyjnej zgłaszającej uwagę	Uzasadnienie*
Wykaz wprowadzonych uwag			
1.			
2.			
3.			
Wykaz uwag częściowo uwzględnionych*			
1.			
2.			
3.			
Wykaz uwag nieuwzględnionych*			
1.			
2.			
3.			

Sporządził: ……..……..

(data, imię i nazwisko)

Sprawdził: ……..…….……..

(data, imię i nazwisko)

Zatwierdził: ……..……..

(data, imię i nazwisko)

* W rubryce „Uzasadnienie” AP zamieszcza informację, dlaczego zmiana nie została uwzględniona lub została uwzględniona tylko w części.

Załącznik nr 3

KARTA AKTUALIZACJI KP/KPH

Lp.	Przyczyna zmiany[1]	Miejsce wprowadzenia zmiany[2]	Numer i tytuł KP, na którą ma wpływ proponowana zmiana oraz propozycja zmiany zapisu[3]
1.			
2.			

Sporządził: .....
(data, imię i nazwisko)
Sprawdził: .....
(data, imię i nazwisko)
Zatwierdził: .....
(data, imię i nazwisko)

[1] Należy podać przyczynę zmiany, np. zmiany legislacyjne, zmiany systemu informatycznego, zalecenia audytowe i kontrolne, uwagi komórki organizacyjnej Centrali ARiMR/SW wraz z następującymi informacjami:

- w przypadku, gdy zmiana KP/KPH wynika ze zmiany legislacji należy podać pełną nazwę ustawy, rozporządzenia itp. oraz jednostki redakcyjnej, która wprowadza daną zmianę, tj. art., ust., pkt, lit.;
- w przypadku, gdy zmiana KP/ KPH wynika ze zmiany systemu teleinformatycznego lub istnieje potrzeba modyfikacji systemu IT należy podać numer konkretnego zgłoszenia zmiany do systemu, jeżeli jest nadany numer propozycji lub pisma - wniosku o dokonanie zmiany systemu;
- w przypadku zaleceń audytowych lub kontrolnych należy powołać się na zalecenie (data, strona, treść zalecenia);

w przypadku uwag komórki organizacyjnej Centrali ARiMR/SW należy powołać się na pismo (pismo znak:..., data, treść uwagi)..

[2] Należy podać miejsce wprowadzenia zmiany w przypadku KP/KPH: tj. rozdział, nr strony, regułę, punkt, w przypadku załącznika: nazwę, symbol, nr strony.

[3] Należy podać numer i tytuł KP/KPH, na którą ma wpływ proponowana zmiana. Należy jednoznacznie określić, w jaki sposób proponowana zmiana wpływa na KP/KPH i jakich zmian należy w niej dokonać, w celu zapewnienia spójności między dwoma KP. Jeżeli proponowana zmiana nie ma wpływu na inne KP/KPH, w niniejszej rubryce należy wpisać słowa „zmiana nie ma wpływu na inne KP/KPH”.