Załącznik nr 14 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Spis treści:

Rozdział 1
Definicje

§ 1.

Użyte w regulaminie określenia oznaczają:

1) Administrator danych – Agencja Restrukturyzacji i Modernizacji Rolnictwa;
2) UODO – Urząd Ochrony Danych Osobowych;
3) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
4) RODO - Rozporządzenie Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
5) Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
6) Inspektor Ochrony Danych (IOD) – wyznaczony przez Administratora danych pracownik realizujący zadania, o których mowa w art. 39 RODO;
7) Właściciel zbioru – dyrektor komórki organizacyjnej w Centrali Agencji, któremu powierzono zbiór danych osobowych;
8) Współadministrator – administrator, który wspólnie z innym lub innymi administratorami ustala cele i sposoby przetwarzania. W drodze wspólnych uzgodnień współadministratorzy określają zakres swojej odpowiedzialności, dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba, że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo krajowe, któremu administratorzy ci podlegają;
9) Przedstawiciel administratora – osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora na mocy art. 27 do reprezentowania administratora w zakresie jego obowiązków wynikających z RODO;
10) Podmiot przetwarzający – podmiot przetwarzający dane osobowe na podstawie umowy lub innego instrumentu prawnego w imieniu Administratora danych, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób których dane dotyczą;
11) Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
12) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych;
13) Privacy by design – zasady ochrony danych osobowych na etapie projektowania systemu służącego do przetwarzania danych osobowych;
14) Privacy by default – zasady ochrony danych osobowych w zakresie podstawowym (domyślne);
15) Privacy Impact Assessment – ocena skutków dla ochrony danych osobowych;

16) Osoba, której dane dotyczą – każda osoba fizyczna, których dane są przetwarzane przez Administratora danych;

17) Prawa osób, których dane dotyczą – prawa, o których mowa w art. 15-21 RODO;

18) Nowy Projekt – każda nowa inicjatywa, której realizacja będzie wiązać się z przetwarzaniem danych osobowych. Nowym projektem będzie w szczególności: zorganizowanie konkursu, stworzenie nowej lub modyfikacja istniejącej aplikacji, wdrożenie nowej lub modyfikacja istniejącej usługi, jeśli w ramach jej świadczenia będzie dochodzić do przetwarzania danych, lub wdrożenie nowego procesu przetwarzania danych osobowych.

Rozdział 2
Cel przetwarzania danych osobowych

§ 2.

1. Agencja przetwarza dane osobowe w celu realizacji zadań określonych w ustawie o Agencji Restrukturyzacji i Modernizacji Rolnictwa oraz w związku z wykonywaniem innych ustaw.
2. Dane osobowe są przetwarzane do czasu realizacji celu, dla którego zostały pozyskane, chyba, że przepisy innych ustaw stanowią inaczej.
3. Niniejszy regulamin ma zastosowanie do danych osobowych przetwarzanych we wszystkich zasobach Agencji, a w szczególności w systemach teleinformatycznych, poza systemami teleinformatycznymi oraz na wszelkich nośnikach danych.

Rozdział 3
Organizacja bezpieczeństwa

§ 3.

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

§ 4.

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

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

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

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

   b) metodologię przeprowadzania oceny skutków dla ochrony danych,

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

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

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

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

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

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

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

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

10) prowadzenie rejestru naruszeń ochrony danych osobowych.

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

§ 5.

1. Każdy zbiór danych osobowych przetwarzanych w Agencji posiada Właściciela zbioru ustanowionego w formie zarządzenia.
2. Właściciel zbioru odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności odpowiada za:
   1) przetwarzanie danych osobowych zgodne z zasadami określonymi w art. 5 RODO, tj.:
      a) zasadą legalności, rzetelności i przejrzystości danych – przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Właściciel zbioru zapewnia przejrzystość przetwarzania danych, w szczególności poprzez informowanie osób, których dane dotyczą o przetwarzaniu danych z chwilą ich pozyskania, w tym o celu i podstawie prawnej przetwarzania. Właściciel zbioru zapewnia, aby dane były zbierane tylko w zakresie niezbędnym do wskazanego celu i przetwarzane tylko przez okres, w jakim jest to niezbędne,
      b) zasadą celowości (ograniczenia celu) – dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami,
      c) zasadą adekwatności (minimalizacji danych) – dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
      d) zasadą merytorycznej poprawności (prawidłowości danych) – dane osobowe powinny być merytorycznie poprawne, a ich zakres i rodzaj adekwatny do celu, w jakim są przetwarzane, oraz w razie potrzeby uaktualniane. Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania powinny zaś zostać niezwłocznie usunięte lub sprostowane,
      e) zasadą ograniczenia czasowego (ograniczenia przechowywania) – dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Właściciel zbioru po osiągnięciu celów przetwarzania danych powinien usunąć te dane albo je zanonimizować,
      f) zasadą zabezpieczenia danych (integralności i poufności danych) – dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

      Zasady, o których mowa w pkt 1 lit. a – f powinny być spełnione łącznie, a Właściciel zbioru jest odpowiedzialny za ich przestrzeganie. Mając na względzie „zasadę rozliczalności", o której mowa w ust. 2 art. 5 RODO, Właściciel zbioru powinien być w stanie wykazać ich przestrzeganie;
   2) prowadzenie w formie papierowej lub w formie elektronicznej rejestru czynności przetwarzania danych osobowych, którego jest właścicielem, zawierającego:
      a) nazwę oraz dane kontaktowe Administratora danych oraz wszelkich współadministratorów, a także Inspektora Ochrony Danych,
      b) cele przetwarzania,
      c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,

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

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

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

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

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

4) nadawanie upoważnień do przetwarzania danych osobowych;

5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

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

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

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

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

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

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

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

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

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

2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

3) gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji

międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

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

§ 6.

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

§ 7.

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

§ 8.

Do obowiązków Inspektora Bezpieczeństwa Informacji w OR należy w szczególności:

1) rozpatrywanie wniosków o udostępnienie danych osobowych;
2) dokonywanie wpisów w ewidencji udostępnień danych osobowych w systemie teleinformatycznym;
3) przechowywanie i aktualizacja wykazu umów powierzenia przetwarzania danych osobowych;

4) przechowywanie aktualnego wykazu osób wyznaczonych do rozpatrywania wniosków o udostępnianie danych osobowych w biurach powiatowych oraz dokumentacji szkoleń przeprowadzonych dla tych osób zawierającej m.in. prezentację na szkolenie i listy obecności uczestników;

5) przechowywanie dokumentacji szkoleń, o których mowa w § 15 ust. 4 przeprowadzonych dla kierowników biur powiatowych, zawierającej m.in. prezentację na szkolenie i listy obecności uczestników.

§ 9.

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

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

5. Dyrektor komórki ds. bezpieczeństwa może wyznaczać dyrektorowi oddziału regionalnego zadania i żądać wyjaśnień w tym zakresie, wydawać polecenia, a także żądać informacji i opinii dotyczących przestrzegania polityki ochrony danych osobowych.
6. Upoważnienie do realizacji czynności audytowych/przeglądów Inspektorom Bezpieczeństwa Informacji w Centrali/oddziale regionalnym wydaje odpowiednio:
   1) Prezes ARiMR;
   2) dyrektor oddziału regionalnego.

Rozdział 4

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

§ 10.

1. Obszar przetwarzania danych osobowych w Agencji stanowi wykaz adresów obiektów:
   1) w których są przetwarzane dane osobowe przez Agencję;
   2) stanowiących lokalizację Równoległego Ośrodka Przetwarzania Danych;
   3) stanowiących lokalizację Centrum Przetwarzania Danych.
2. Wykaz adresów obiektów stanowiących obszar przetwarzania danych osobowych na druku stanowiącym załącznik nr 1 do niniejszego regulaminu, w terminie do dnia 31 grudnia każdego roku kalendarzowego, dostarcza dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych:
   1) Administrator Zabezpieczeń Fizycznych w Centrali Agencji – w odniesieniu do obiektów (budynków) Centrali, oddziałów regionalnych i biur powiatowych,
   2) Administrator Systemu - w odniesieniu do Centrum Przetwarzania Danych i Równoległego Ośrodka Przetwarzania Danych.
3. Osoby wymienione w ust. 2 pkt 1 i 2 informują dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących lokalizacji obszarów przetwarzania w terminie 7 dni od wystąpienia zmiany.
4. Administrator Systemu sporządza:
   1) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
   2) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, który może być sporządzony w wersji elektronicznej;
   3) informację o sposobie przepływu danych pomiędzy poszczególnymi systemami;
   4) opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
5. Środki techniczne i organizacyjne dobierane są adekwatnie do rodzaju danych, okoliczności ich przetwarzania oraz ryzyka naruszeń ochrony.

6. Administrator Systemu aktualizuje informacje, o których mowa w ust. 4 pkt 1 – 4 w terminie 7 dni od wystąpienia zmian i przesyła aktualne wersje dyrektorowi komórki ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych.

§ 11.

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

Rozdział 5
Tworzenie i usuwanie zbiorów danych osobowych

§ 12.

1. Właściciel zbioru zobowiązany jest zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o utworzeniu nowego zbioru nie później niż w terminie 7 dni od rozpoczęcia tworzenia zbioru.
2. Zawiadomienie następuje przez przesłanie informacji w zakresie:
   1) nazwy zbioru danych osobowych;
   2) podstawy prawnej przetwarzania;
   3) celu przetwarzania;
   4) opisu kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   5) kategorii odbiorców, którym dane osobowe zostaną ujawnione, w tym odbiorców państw trzecich lub w organizacjach międzynarodowych;
   6) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
   7) planowanych terminów usunięcia poszczególnych kategorii danych;

8) ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO uwzględniających ryzyko przetwarzania danych w zgłaszanym zbiorze.

3. Na wniosek Właściciela zbioru, w przypadku tworzenia nowego zbioru Administrator Systemu określa warunki techniczne dotyczące zabezpieczeń zbioru w systemie teleinformatycznym.
4. Właściciel zbioru jest zobowiązany zawiadomić dyrektora komórki ds. bezpieczeństwa oraz Inspektora Ochrony Danych o wszelkich zmianach dotyczących przetwarzania danych osobowych w zbiorze nie później niż w terminie 14 dni od ich wystąpienia.
5. Administrator Systemu jest zobowiązany zgłosić Właścicielowi zbioru wszelkie zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczenia w systemie teleinformatycznym w ciągu 7 dni od daty zaistnienia tych zmian.

§ 13.

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

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

§ 14.

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

§ 15.

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

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

§ 16.

1. Upoważnienie do przetwarzania danych w zbiorach (upoważnienie szczególne) może być nadane:

1) osobom zatrudnionym (wykonującym pracę) w Agencji bez względu na podstawę prawną zatrudnienia, jeżeli uzyskały one upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne);

2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia; osobom tym można nadać upoważnienie bez obowiązku uprzedniego uzyskania upoważnienia ogólnego.

2. Upoważnienie do przetwarzania danych w zbiorach przetwarzanych w systemie informatycznym jest nadawane w wyniku zaakceptowania przez Właściciela zbioru wniosku o nadanie uprawnień do pracy w systemie. Druk wniosku określono w Książce procedur KP-611-101-ARiMR „Obsługa kont użytkowników systemów informatycznych ARiMR".

3. Wobec zbiorów przetwarzanych w systemie informatycznym w Centrali Agencji, z wnioskiem o nadanie uprawnień do pracy w systemie występują osoby określone w KP-611-101-ARiMR.

4. Wniosek o nadanie uprawnień do pracy w systemie jest zatwierdzany przez wszystkich Właścicieli zbiorów, do których zbiorów danych osobowych będzie miała dostęp osoba, której zostaną nadane uprawnienia, z zastrzeżeniem ust. 7.

5. Wniosek o nadanie uprawnień po uprzednim zatwierdzeniu przez Właściciela(i) zbioru(ów), realizuje Administrator Systemu.

6. Zbiór wszystkich zrealizowanych wniosków o nadanie uprawnień do pracy w systemie informatycznym, przechowywany przez Administratora Systemu, jest częścią ewidencji osób upoważnionych.

7. Wobec zbiorów przetwarzanych w systemie informatycznym w oddziałach regionalnych i biurach powiatowych Agencji wniosek o nadanie uprawnień do pracy w systemie, w mieniu Właścicieli zbiorów, zatwierdza dyrektor oddziału regionalnego.

8. Wniosek o nadanie uprawnień zatwierdzony przez dyrektora oddziału regionalnego lub osobę przez niego upoważnioną jest przechowywany w oddziale regionalnym w dokumentacji pracowniczej osoby uprawnionej.

9. Zbiór wszystkich wniosków zrealizowanych w oddziale regionalnym o nadanie uprawnień do pracy w systemie, przechowywany w oddziale regionalnym, jest częścią ewidencji osób upoważnionych.

10. Upoważnienie do przetwarzania danych osobowych w zbiorach przetwarzanych wyłącznie w formie papierowej nadają:

    1) w Centrali Agencji – Właściciel zbioru;

    2) w oddziale regionalnym i biurze powiatowym – dyrektor oddziału regionalnego.

11. Upoważnienie, o którym mowa w ust. 10 nadawane jest poprzez zatwierdzenie wniosku sporządzonego na druku stanowiącym załącznik nr 4 do niniejszego Regulaminu.

12. Do sporządzania wniosku, o którym mowa w ust. 10, stosuje się odpowiednio zasady kompetencyjne obowiązujące przy sporządzaniu wniosku o nadanie uprawnień do przetwarzania danych w systemie informatycznym.

13. Zatwierdzone wnioski o nadanie upoważnienia do przetwarzania danych w zbiorach przetwarzanych wyłącznie w formie papierowej są przechowywane odpowiednio przez Właścicieli zbiorów w Centrali Agencji i przez dyrektorów oddziałów regionalnych. Są one częścią ewidencji osób upoważnionych.

§ 17.

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

Rozdział 7
Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 18.

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

Rozdział 8
Realizacja praw osób, których dane dotyczą

§ 19.

1. Każdej osobie przysługuje prawo dostępu do danych osobowych, które jej dotyczą oraz do wydania kopii danych, sprostowania danych, usunięcia danych („prawo do bycia zapomnianym”), ograniczenia przetwarzania, przeniesienia danych oraz prawo do sprzeciwu, zgodnie z art. 15-21 RODO.

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

Rozdział 9
Udostępnianie danych osobowych

§ 20.

1. Dane osobowe udostępniane są na wniosek.
2. Wniosek o udostępnienie danych osobowych, który wpłynął do biura powiatowego lub oddziału regionalnego załatwia dyrektor oddziału regionalnego.

3. Wniosek o udostępnienie danych osobowych, który z przyczyn formalnych lub merytorycznych nie może zostać załatwiony przez dyrektora oddziału regionalnego, załatwia Właściciel zbioru.
4. Wnioski o udostępnienie danych osobowych załatwiane przez dyrektora oddziału regionalnego rozpatruje Inspektor Bezpieczeństwa Informacji w OR. W tym celu m.in.:
   1) dokonuje oceny wniosków pod względem formalnym i merytorycznym;
   2) przygotowuje projekty pism w sprawie usunięcia nieprawidłowości, uzupełnienia wniosków, udzielenia niezbędnych wyjaśnień oraz projekty odpowiedzi na wnioski, które przedkłada do podpisu dyrektorowi oddziału regionalnego;
   3) występuje do komórek organizacyjnych oddziału regionalnego lub biura powiatowego o przekazanie informacji merytorycznej niezbędnej do przygotowania odpowiedzi na wnioski; za terminowość i integralność przekazanej informacji odpowiedzialność ponosi kierownik biura powiatowego lub kierownik komórki organizacyjnej oddziału regionalnego przekazujący informację.
5. Osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym opiniuje projekt pisma w sprawie usunięcia nieprawidłowości, uzupełnienia wniosku lub udzielenia niezbędnych wyjaśnień oraz projekt odpowiedzi na wniosek, jeżeli taki projekt zostanie mu przedstawiony do zaopiniowania przez Inspektora Bezpieczeństwa Informacji w OR; akceptując projekt pisma, osoba zatrudniona na stanowisku Radcy prawnego w oddziale regionalnym składa na nim czytelny podpis.
6. Wniosek o udostępnienie danych osobowych z Systemu Identyfikacji i Rejestracji Zwierząt, od osoby zatrudnionej w Inspekcji Weterynaryjnej, który wpłynął do biura powiatowego załatwia kierownik biura powiatowego.
7. Kierownik biura powiatowego zgłasza do dyrektora oddziału regionalnego wykaz osób wyznaczonych do rozpatrywania wniosków o udostępnienie danych i odpowiada za jego aktualizację. Osoby te podlegają co najmniej raz w roku szkoleniom doskonalącym prowadzonym przez Inspektorów Bezpieczeństwa Informacji z OR.
8. Wniosek o udostępnienie danych osobowych załatwiany w biurze powiatowym, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany do oddziału regionalnego w celu uzyskania opinii Inspektora Bezpieczeństwa Informacji w OR. Do kopii wniosku dołącza się informacje niezbędne do jego rozpatrzenia oraz stanowisko kierownika BP.
9. Wniosek, który wpłynął do Centrali Agencji załatwia Właściciel zbioru. Wniosek organu egzekucyjnego może zostać przekazany przez Właściciela zbioru do załatwienia dyrektorowi oddziału regionalnego.
10. Właściciel zbioru jest obowiązany wyznaczyć co najmniej dwie osoby do rozpatrywania wniosków o udostępnienie danych (osoby wyznaczone), o których informuje dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych. Tylko osoby wyznaczone rozpatrują wnioski o udostępnienie danych osobowych, które załatwia Właściciel zbioru.
11. Dyrektor komórki właściwej ds. bezpieczeństwa prowadzi wykaz osób wyznaczonych, które podlegają okresowemu szkoleniu. Za przekazywanie informacji niezbędnych do prowadzenia aktualnego wykazu odpowiadają Właściciele zbiorów.

12. Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi. Projekt odpowiedzi przesłany z oddziału regionalnego wymaga podpisu osoby zatrudnionej na stanowisku radcy prawnego.
13. Dane osobowe udostępnia się na wniosek sporządzony w formie pisemnej, spełniający wymagania formalne, określone w przepisach prawa. Szczegółowe zasady postępowania przy rozpatrywaniu wniosków o udostępnienie danych osobowych określają „Wytyczne dotyczące rozpatrywania wniosków o udostępnienie danych osobowych". Obowiązujące Wytyczne są opracowywane i udostępniane, a w razie konieczności aktualizowane przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
14. Informacje zawierające dane osobowe są udostępniane uprawnionym podmiotom:
    1) w formie pisemnego wydruku, listem poleconym lub za potwierdzeniem osobistego odbioru;
    2) za pomocą elektronicznej skrzynki podawczej e-PUAP – z użyciem podpisu kwalifikowanego lub potwierdzonego profilem zaufanym;
    3) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych);
    4) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru;
    5) w inny sposób określony przepisami prawa lub umową.
15. Podstawową formą przekazywania danych osobowych jest metoda określona w ust. 14 pkt 1.
16. W szczególnie uzasadnionych przypadkach stosuje się metody określone w ust. 14 pkt 2 – 5. Uzasadnienie takiego przypadku, sporządzone na piśmie, dołącza się do akt sprawy.
17. Zawartość elektronicznych nośników informacji podlega kontroli i pisemnej akceptacji bezpośredniego przełożonego - osoby przygotowującej informację określoną w ust. 14.
18. Jeżeli tryb udostępniania danych osobowych określa umowa, przepisów niniejszego rozdziału nie stosuje się w zakresie postanowień umowy.
19. Ewidencja przypadków udostępnienia danych prowadzona jest w wyznaczonym systemie informatycznym. Ewidencję prowadzą:
    1) w Centrali Agencji – Właściciel zbioru;
    2) w oddziale regionalnym – dyrektor;
    3) w biurze powiatowym – kierownik.

Rozdział 10
Powierzanie przetwarzania danych osobowych innym podmiotom

§ 21.

1. Powierzenie przetwarzania danych nie wyłącza, ani nie ogranicza odpowiedzialności Właściciela zbioru/dyrektora oddziału regionalnego za zgodne z prawem przetwarzanie tych danych.

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

7. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w OR Agencji, której realizacja może wiązać się z przetwarzaniem powierzonych danych osobowych, wymaga akceptacji w wyniku złożenia czytelnych podpisów przez:
   1) Dyrektora OR;
   2) kierownika komórki organizacyjnej przygotowującej projekt;
   3) Inspektora Bezpieczeństwa Informacji w OR;
   4) osoby zajmującej samodzielne stanowisko radcy prawnego w OR.
8. Właściciel zbioru nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w Centrali i wykonywanych na terenie właściwości Centrali Agencji. Dyrektor oddziału regionalnego nadzoruje wykonywanie umów powierzenia przetwarzania danych osobowych zawartych w oddziale regionalnym oraz wszystkich umów wykonywanych na terenie właściwości oddziału regionalnego chyba, że Właściciel zbioru postanowi inaczej.
9. Właściciele zbiorów i dyrektorzy oddziałów regionalnych prowadzą wykaz umów powierzenia przetwarzania danych według wzoru stanowiącego załącznik nr 6 do niniejszego regulaminu.

Rozdział 11
Postępowanie w przypadku kontroli PUODO

§ 22.

1. PUODO lub upoważnieni przez PUODO pracownicy UODO, zwani dalej „kontrolującymi", mają prawo do przeprowadzania kontroli w Agencji. Kontrolę przeprowadza się po okazaniu przez kontrolującego imiennego upoważnienia wraz z legitymacją służbową. Imienne upoważnienie do przeprowadzania kontroli powinno zawierać elementy wskazane w art. 81 ust. 2 Ustawy.
2. Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli (przedstawiciela kontrolowanej komórki lub jednostki organizacyjnej). Szczegółowe warunki i zasady przeprowadzania kontroli określa Ustawa.
3. Inspektor Ochrony Danych jest zawiadamiany bez zbędnej zwłoki o kontroli PUODO w Agencji i może być obecny podczas wykonywania przez kontrolujących czynności kontrolnych w Agencji.
4. Właściciel zbioru, Administrator Systemu, Administrator Zabezpieczeń Fizycznych, dyrektor oddziału regionalnego, kierownik biura powiatowego i inne osoby poddawane kontroli zobowiązani są do ścisłej współpracy z Inspektorem Ochrony Danych.
5. Inspektor Ochrony Danych zapewnia pod względem organizacyjnym warunki niezbędne do przeprowadzenia kontroli PUODO w Centrali Agencji.
6. Merytoryczną obsługę kontroli PUODO polegającą m.in. na udzieleniu kontrolującym niezbędnych informacji, wyjaśnień, dostępu do dokumentów i systemów teleinformatycznych w Centrali Agencji zapewniają w granicach swoich kompetencji i uprawnień:
   1) Właściciel zbioru wobec powierzonych mu zbiorów;

2) Administrator Systemu;
3) Administrator Zabezpieczeń Fizycznych;
4) Inspektor Ochrony Danych;
5) dyrektor komórki właściwej ds. bezpieczeństwa;
6) kierownik komórki organizacyjnej, w której są przetwarzane dane osobowe;
7) pracownicy i inne osoby wykonujące pracę na rzecz Agencji w odniesieniu do wykonywania obowiązków związanych z przetwarzaniem danych osobowych, tylko w obecności przełożonego lub osoby nadzorującej ich pracę.

7. Dyrektor oddziału regionalnego zapewnia warunki i obsługę kontroli PUODO w oddziale regionalnym.
8. Merytoryczną obsługę kontroli PUODO w oddziale regionalnym zapewniają kierownicy jednostek i komórek organizacyjnych w granicach swoich kompetencji i uprawnień. Pracownicy i inne osoby wykonujące pracę w oddziale regionalnym, związaną z przetwarzaniem danych osobowych, uczestniczą w czynnościach kontrolnych tylko w obecności przełożonego lub osoby nadzorującej ich pracę.
9. W trakcie czynności kontrolnych wykonywanych przez kontrolujących w oddziale regionalnym uczestniczy Inspektor Bezpieczeństwa Informacji z OR. Dyrektor oddziału regionalnego może wyznaczyć też inne osoby, które będą brały udział w tych czynnościach.
10. Kierownicy komórek organizacyjnych w oddziale regionalnym, kierownicy biur powiatowych i inne osoby poddawane kontroli są zobowiązane do ścisłej współpracy z Inspektorem Bezpieczeństwa Informacji w OR oraz innymi osobami wyznaczonymi przez dyrektora oddziału regionalnego.

Rozdział 12
Odpowiedzialność za naruszenie zasad ochrony danych osobowych

§ 23.

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

Załącznik nr 1 do Regulaminu ochrony danych osobowych.

Znak sprawy:

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

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

Nazwa obiektu	Województwo	Powiat	Adres

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

..…….., dnia……..… r.
(miejscowość, data)

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) (Dz. Urz. UE L 119 z 04.05.2016 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem", upoważniam:

Panią/Pana*……
……..,

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

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

w zakresie niezbędnym do wykonywania powierzonej pracy***.

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

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

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

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

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

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

Pouczenie:

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

** **należy zaznaczyć obydwa checkbox-y jedynie w przypadku, gdy zakres czynności obejmuje przetwarzanie danych osobowych zwykłych i przetwarzanie danych osobowych szczególnych kategorii, o których mowa w art. 9 Rozporządzenia, tj. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej. W pozostałych przypadkach należy zaznaczyć jedynie checkbox dotyczący danych osobowych zwykłych i przekreślić checkbox dotyczący danych szczególnych kategorii.**

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

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

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

Załącznik nr 4 do Regulaminu ochrony danych osobowych

Znak sprawy:

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH
w zbiorach przetwarzanych w formie papierowej

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) (Dz. Urz. UE L 119 z 04.05.2016 r., s. 1 oraz Dz. Urz. UE. L 127 z 23.05.2018 r., str. 2) zwanego dalej: „Rozporządzeniem",

upoważniam / odbieram upoważnienie*:

Panią/Pana*……..,

posiadającą/ego nr. KIP – ……..,

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

do przetwarzania danych osobowych w zbiorze:

……

……

w następującym zakresie:

……

……

……

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

* Niepotrzebne skreślić

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

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