Załącznik nr 14 do zarządzenia Nr 40/2008

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

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Spis treści

Rozdział 1
Definicje

§ 1.

Użyte w regulaminie określenia oznaczają:

1) *(skreślony)*

2) **Administrator danych** – Agencję Restrukturyzacji i Modernizacji Rolnictwa,

3) **GIODO** – Generalnego Inspektora Ochrony Danych Osobowych,

4) **Ustawa** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

5) **Właściciel zbioru** – dyrektora komórki organizacyjnej w Centrali Agencji, któremu powierzono zbiór danych osobowych,

6) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Rozdział 2
Cel przetwarzania danych osobowych

§ 2.

1. Agencja przetwarza dane osobowe w celu prowadzenia działalności określonej 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. Właściciel zbioru wykonuje obowiązki administratora danych wobec powierzonego mu zbioru danych osobowych za wyjątkiem tych obowiązków, które zostały przekazane innym podmiotom.
2. 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.

3. Szczegółowe zakresy obowiązków i odpowiedzialności Właściciela Zasobu ustanowione w zarządzeniu Prezesa ARiMR w sprawie bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do Właściciela zbioru.
4. Właściciel zbioru nie może delegować swoich zadań do podmiotów zewnętrznych.
5. Dyrektor oddziału regionalnego nie jest Właścicielem zbioru.

§ 4.

1. Do zadań dyrektora komórki właściwej ds. bezpieczeństwa informacji należy opracowanie i aktualizacja polityki ochrony danych osobowych oraz dokonywanie jej wykładni. Dyrektor wykonuje swoje zadania poprzez:
   1) określenie zasad przetwarzania danych osobowych m.in. ich udostępniania i powierzania, a także zasad ochrony danych osobowych i zarządzania danymi osobowymi,
   2) określenie jednolitego dla całej Agencji sposobu prowadzenia dokumentacji, o której mowa w przepisach o ochronie danych osobowych oraz dokumentowania wykonania czynności wymaganych przez te przepisy,
   3) dokonywanie wykładni polityki ochrony danych osobowych m.in. przez sporządzanie opinii i przedstawianie stanowiska w sprawie stosowania obowiązującego w tym zakresie prawa,
   4) prowadzenie szkoleń dotyczących stosowania polityki ochrony danych osobowych,
   5) tworzenie i aktualizację procedur oraz innych dokumentów wynikających z zadań powierzonych w polityce ochrony danych osobowych,
   6) opiniowanie, pod względem zgodności z polityką ochrony danych osobowych, umów, procedur i innych dokumentów wytworzonych w Agencji, dotyczących bezpieczeństwa i przetwarzania danych osobowych,
   7) weryfikację wniosków o rejestrację zbiorów danych osobowych i wniosków zawierających zgłoszenie zmian w zbiorze danych oraz wniosków o wykreślenie zbioru z rejestru,
   8) przechowywanie dokumentacji stanowiącej politykę bezpieczeństwa, o której mowa w przepisach wykonawczych do Ustawy, a którą tworzą informacje otrzymywane od Właścicieli zbiorów, Administratora Systemu i Administratora Zabezpieczeń Fizycznych,
   9) reprezentowanie Agencji jako Administratora danych w:
      – postępowaniach administracyjnych prowadzonych przez GIODO,
      – sprawach przetwarzania i ochrony danych osobowych w zakresie udzielonych upoważnień.
2. *(skreślony)*

§ 5.

1. Każdy zbiór danych osobowych przetwarzanych w Agencji posiada Właściciela zbioru ustanowionego w formie zarządzenia. Projekt zarządzenia sporządza dyrektor komórki

organizacyjnej właściwy do objęcia właścicielstwa tego zbioru, w terminie 7 dni od rozpoczęcia tworzenia zbioru.

2. Właściciel zbioru odpowiada za realizację ustawowych obowiązków Administratora danych, a w szczególności odpowiada za:
   1) zgodne z prawem 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) przechowywanie danych osobowych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne,
   4) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane i/lub udostępniane,
   5) nadawanie upoważnień do przetwarzania danych osobowych,
   6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   7) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
   8) nadzorowanie systemów teleinformatycznych służących do przetwarzania powierzonych zbiorów danych osobowych za pośrednictwem Administratora Systemu,
   9) zgłaszanie zbiorów danych osobowych do rejestracji w GIODO i aktualizacja zgłoszeń, udzielanie wyjaśnień GIODO,
   10) reprezentowanie administratora danych wobec powierzonych zbiorów w czasie kontroli prowadzonej przez GIODO,
   11) terminowe przekazywanie dyrektorowi komórki właściwej ds. bezpieczeństwa informacji – informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych zadań,
   12) zapewnienie warunków i pomocy osobom dokonującym kontroli,
   13) udzielanie informacji osobom, których dane są przetwarzane.

§ 6.

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

§ 7.

1. Dyrektor oddziału regionalnego wykonuje wyznaczone obowiązki Właściciela zbioru wobec zbiorów przetwarzanych w oddziale regionalnym.
2. 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 zgodne z prawem przetwarzanie tych danych.
3. Obowiązki Właściciela zasobu i przypisana mu odpowiedzialność, ustanowione w zarządzeniu Prezesa ARiMR w sprawie bezpieczeństwa informacji w ARiMR stosuje

się odpowiednio do dyrektora oddziału regionalnego administrującego w oddziale regionalnym zbiorami danych osobowych.

4. Dyrektor oddziału regionalnego w szczególności jest zobowiązany do:
   1) nadawania upoważnień do przetwarzania danych osobowych i prowadzenia ewidencji osób upoważnionych,
   2) załatwiania wniosków o udostępnienie danych,
   3) zawierania umów powierzenia przetwarzania danych realizowanych w oddziale regionalnym,
   4) terminowego przekazywania dyrektorowi komórki właściwej ds. bezpieczeństwa informacji - informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych zadań,
   5) zapewnienia warunków i pomocy osobom dokonującym kontroli w oddziale regionalnym i podległych biurach powiatowych.

§ 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 właściwej ds. bezpieczeństwa informacji nadzoruje przestrzeganie w Agencji polityki ochrony danych osobowych, w tym stosowanie obowiązujących środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.
2. Nadzorowanie przestrzegania polityki ochrony danych osobowych następuje m.in. przez wykonywanie czynności kontrolnych, 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. Realizując uprawnienie określone w ust. 1 dyrektor komórki właściwej ds. bezpieczeństwa informacji w szczególności:
   a) kontroluje sposób przetwarzania danych osobowych we wszystkich komórkach i jednostkach organizacyjnych Agencji,

b) kontroluje sposób przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych we wszystkich komórkach i jednostkach organizacyjnych Agencji,

c) prowadzi szkolenia dotyczące przestrzegania polityki ochrony danych osobowych w Agencji.

3a. 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 w zakresie:

a) kontrolowania sposobu przetwarzania danych osobowych w Agencji,

b) kontrolowania sposobu przestrzegania obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji,

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

3b. 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 zadania w zakresie:

a) kontrolowania sposobu przetwarzania danych osobowych w oddziale regionalnym i biurach powiatowych,

b) kontrolowania przestrzegania w oddziale regionalnym i biurach powiatowych obowiązujących standardów ochrony danych osobowych w odniesieniu do zastosowanych środków technicznych i organizacyjnych,

c) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w oddziale regionalnym i biurach powiatowych.

4. *(skreślony)*

5. Realizując uprawnienie, o którym mowa w ust. 1 dyrektor komórki właściwej ds. bezpieczeństwa informacji 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 kontroli Inspektorom Bezpieczeństwa Informacji w Centrali/oddziale regionalnym wydaje odpowiednio:

a) Prezes ARiMR,

b) dyrektor oddziału regionalnego.

7. Obowiązujący wzór upoważnienia do kontroli zawiera zarządzenie Prezesa ARiMR w sprawie wprowadzenia Regulaminu Kontroli w Agencji Restrukturyzacji i Modernizacji Rolnictwa.

Rozdział 4
Prowadzenie dokumentacji polityki 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 dostarcza dyrektorowi komórki właściwej ds. bezpieczeństwa informacji:
   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,

   w terminie do dnia 31 grudnia każdego roku kalendarzowego.
3. Osoby wymienione w ust. 2 pkt 1 i 2 informują dyrektora komórki właściwej ds. bezpieczeństwa informacji 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, zgodny z treścią umieszczoną w części E wniosku zgłoszenia zbioru.
5. Środki techniczne i organizacyjne dobierane są w oparciu o wysoki poziom bezpieczeństwa, o którym mowa w rozporządzeniu wykonawczym do Ustawy.
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 właściwej ds. bezpieczeństwa informacji.
7. Wykaz i informacje, o których mowa w ust. 1–4 składają się na dokumentację polityki bezpieczeństwa danych osobowych.

§11.

1. Dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, o której mowa w rozporządzeniu wykonawczym do Ustawy, zawiera

opis sposobu realizacji wymogów ustawowych ustanowionych dla systemów informatycznych przetwarzających dane osobowe.

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 informacji aktualną wersję Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Administrator Systemu zapewnia realizację wymogów dotyczących funkcjonalności aplikacji służących do przetwarzania danych osobowych.
5. Właściciel zbioru nadzoruje Administratora Systemu w zakresie zapewnienia wymaganych funkcjonalności dla aplikacji służących do przetwarzania zbiorów danych osobowych.
6. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych określa regulamin zarządzania incydentami bezpieczeństwa informacji.

Rozdział 5
Ewidencja, rejestracja i usuwanie zbiorów danych osobowych

§12.

1. Właściciel zbioru podlegającego zgłoszeniu GIODO jest zobowiązany zawiadomić dyrektora komórki właściwej ds. bezpieczeństwa informacji o konieczności zgłoszenia nowego zbioru nie później niż w terminie 7 dni od rozpoczęcia tworzenia zbioru.
2. Zawiadomienie następuje przez przesłanie do dyrektora komórki właściwej ds. bezpieczeństwa informacji wypełnionego wniosku zgłoszenia zbioru danych osobowych wraz z uzasadnieniem. Wniosek przesyła się w dwóch egzemplarzach (oryginał i parafowana kopia).
3. Na wniosek Właściciela zbioru Administrator Systemu określa warunki techniczne dotyczące zabezpieczeń zbioru w systemie teleinformatycznym.
4. Dyrektor komórki właściwej ds. bezpieczeństwa informacji weryfikuje treść wniosku i jego uzasadnienie.
5. Wniosek podpisany przez Administratora danych lub osobę upoważnioną, dyrektor komórki właściwej ds. bezpieczeństwa informacji przekazuje do GIODO, zachowując jego kopię.
6. Kopie wniosków przechowywane przez dyrektora komórki właściwej ds. bezpieczeństwa informacji tworzą ewidencję zbiorów danych osobowych.
7. Właściciel zbioru jest zobowiązany zawiadomić dyrektora komórki właściwej ds. bezpieczeństwa informacji o konieczności zgłoszenia zmian do wniosku zgłoszenia zbioru (aktualizacja wniosku) nie później niż w terminie 14 dni od ich wystąpienia.
8. 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.

9. Aktualizacja wniosku następuje w trybie właściwym dla zgłoszenia nowego zbioru do GIODO.

§13.

1. Wykreślenie zbioru danych osobowych z rejestru GIODO jest dokonywane, w drodze decyzji administracyjnej, jeżeli:
   1) zaprzestano przetwarzania danych w zarejestrowanym zbiorze,
   2) rejestracji dokonano z naruszeniem prawa.
2. Właściciel zbioru decyduje o trwałym usunięciu zbioru danych osobowych po uzyskaniu opinii dyrektora komórki właściwej ds. bezpieczeństwa informacji.
3. Właściciel zbioru podejmuje działania w celu usunięcia zbioru danych osobowych.
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 sporządza wniosek wraz z uzasadnieniem do GIODO o wykreślenie zbioru danych osobowych.
7. Wniosek podpisuje Administrator danych lub osoba upoważniona, po parafowaniu go przez:
   1) Właściciela zbioru,
   2) Administratora Systemu, jeżeli zbiór był przetwarzany w systemie informatycznym,
   3) dyrektora komórki właściwej ds. bezpieczeństwa informacji.
8. Kopia wniosku jest przechowywana w ewidencji zbiorów danych osobowych.

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 w zbiorach oraz poza zbiorami wymaga uzyskania upoważnienia do przetwarzania danych osobowych.
2. Upoważnienie nadaje się przed dopuszczeniem osoby do przetwarzania danych osobowych. Upoważnienie odbiera się niezwłocznie po ustaniu celu, dla którego zostało nadane.

§15.

1. Upoważnienie do przetwarzania danych 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. Dyrektor komórki właściwej ds. bezpieczeństwa informacji przesyła do komórek i jednostek organizacyjnych aktualny 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. Szkolenie prowadzi dyrektor komórki właściwej ds. bezpieczeństwa informacji oraz odpowiednio Inspektor Bezpieczeństwa Informacji w OR, 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.

4a. 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 przenoszone do pracy w Centrali, oddziale regionalnym lub biurze powiatowym,

3) osoby, które w wyniku awansu obejmują stanowisko dyrektora oddziału regionalnego.

5. 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 zarządzenia).

6. Dyrektor komórki właściwej ds. bezpieczeństwa informacji zawiadamia dyrektora komórki właściwej ds. kadrowych w Centrali oraz odpowiednio Inspektor Bezpieczeństwa Informacji w OR - komórkę właściwą ds. kadrowych w oddziale regionalnym, o osobach uczestniczących w szkoleniu podstawowym. Zawiadomienie następuje przez doręczenie wypełnionych oświadczeń sporządzonych na druku stanowiącym załącznik nr 2 do niniejszego regulaminu. Osoby, które nie odbyły szkolenia podstawowego nie mogą zostać dopuszczone do pracy związanej z przetwarzaniem danych osobowych.

7. Osoba przeszkolona podpisuje oświadczenie, w którym 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.

8. Oświadczenie złożone na druku stanowiącym załącznik nr 2 do niniejszego regulaminu jest dołączane do akt osobowych lub podobnych akt prowadzonych dla osób wykonujących pracę w Agencji na innej podstawie niż stosunek pracy.

8a. Kopie list obecności uczestników szkoleń podstawowych przeprowadzanych przez kierowników biur powiatowych oraz oryginały oświadczeń 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 oświadczeń otrzymanych 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 ich sporządzenia.

9. *(skreślony)*

10. *(skreślony)*

11. Upoważnienie do przetwarzania danych osobowych w Centrali, osobom wskazanym w ust. 1, w tym osobom przeniesionym do pracy w Centrali, nadaje dyrektor komórki właściwej ds. kadrowych oraz odpowiednio w oddziale regionalnym i biurach powiatowych - dyrektor oddziału regionalnego, wypełniając druk stanowiący załącznik nr 3 do niniejszego regulaminu. Dyrektorom wszystkich komórek organizacyjnych w Centrali oraz dyrektorom oddziałów regionalnych upoważnienie nadaje Prezes Agencji lub osoba przez niego upoważniona. Upoważnienie przechowuje się w aktach osobowych lub podobnych aktach prowadzonych dla osób wykonujących pracę na innej podstawie niż stosunek pracy.

12. W szczególnie uzasadnionych przypadkach, Dyrektor komórki właściwej ds. kadrowych / dyrektor oddziału regionalnego mogą nadać upoważnienie ogólne osobom wskazanym w ust. 1 pkt 2 bez obowiązku ich przeszkolenia.

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 4 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 przekazanym przez dyrektora komórki właściwej ds. kadrowych, w którym zobowiązują się do zachowania w poufności przetwarzanych danych oraz zastosowanych w Agencji środków ochrony.

16. Oświadczenie sporządzone na druku stanowiącym załącznik nr 2 do niniejszego regulaminu jest przechowywane 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 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.

3a. 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. 6.

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

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

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

7. (skreślony)

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

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. (skreślony)

11. (skreślony)

12. (skreślony)

13. 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,

zatwierdzając wniosek sporządzony na druku stanowiącym załącznik nr 5 do niniejszego regulaminu. Upoważnienie przechowują odpowiednio, Właściciel zbioru oraz dyrektor oddziału regionalnego, w komórce właściwej do spraw obsługi oddziału regionalnego.

14. Do sporządzania wniosku, o którym mowa w ust. 13, stosuje się odpowiednio zasady kompetencyjne obowiązujące przy sporządzaniu wniosku o nadanie uprawnień do przetwarzania danych w systemie informatycznym.

15. (skreślony)

16. (skreślony)

17. 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 następuje w wyniku jego odebrania przez osobę uprawnioną.
3. 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, o której mowa w Ustawie.
2. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Agencji zawiera łącznie:
   1) zbiór osób, które uzyskały upoważnienia do przetwarzania danych osobowych poza zbiorami, 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. *(skreślony)*
4. Administrator Systemu prowadzi ewidencję identyfikatorów użytkowników systemu informatycznego, w którym są przetwarzane dane osobowe.

Rozdział 8
Udzielanie informacji osobom, których dane są przetwarzane

§19.

1. Każdej osobie przysługuje prawo do kontroli sposobu przetwarzania danych osobowych, które jej dotyczą. Osoba zainteresowana może skorzystać z tego prawa, w formie informacji przekazanej przez Agencję, nie częściej niż raz na 6 miesięcy.
2. Na wniosek osoby, której dane dotyczą, Właściciel zbioru w terminie 30 dni informuje osobę o przysługujących jej prawach oraz udziela jej informacji w zakresie wskazanym w Ustawie.
3. Wniosek osoby, której dane są przetwarzane złożony w oddziale regionalnym lub biurze powiatowym rozpatruje Właściciel zbioru. Odpowiedź na wniosek podlega uzgodnieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji.
4. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Właściciel zbioru jest obowiązany, bez zbędnej zwłoki, do przywrócenia zgodnego z prawem przetwarzania danych osobowych.
5. Właściciel zbioru prowadzi postępowanie wyjaśniające i zawiadamia o jego wyniku osobę, która złożyła zastrzeżenia do przetwarzania jej danych osobowych.

Rozdział 9
Udostępnianie danych osobowych

§20.

1. Wniosek o udostępnienie danych osobowych, który wpłynął do biura powiatowego lub oddziału regionalnego załatwia dyrektor oddziału regionalnego.
2. Wniosek o udostępnienie danych osobowych, którego z przyczyn formalnych lub merytorycznych nie może załatwić dyrektor oddziału regionalnego, załatwia Właściciel zbioru.
3. Wnioski o udostępnienie danych osobowych załatwiane przez dyrektora oddziału regionalnego rozpatruje Inspektor Bezpieczeństwa Informacji w OR i 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.

4. Radca prawny 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, radca prawny w oddziale regionalnym składa na nim czytelny podpis.
5. 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.
6. 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.
7. 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.
8. Wniosek, który wpłynął do Centrali Agencji załatwia Właściciel zbioru. Wniosek organu egzekucyjnego może zostać przekazany przez Właściciela zbioru do załatwienia dyrektorowi oddziału regionalnego.
9. 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 informacji. Tylko osoby wyznaczone rozpatrują wnioski o udostępnienie danych osobowych, które załatwia Właściciel zbioru.
10. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi wykaz osób wyznaczonych, które podlegają okresowemu szkoleniu. Za przekazywanie informacji niezbędnych do prowadzenia aktualnego wykazu odpowiadają Właściciele zbiorów.
11. Wniosek o udostępnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany wraz z informacjami niezbędnymi dla jego rozpatrzenia, do dyrektora komórki właściwej ds. bezpieczeństwa informacji w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi. Projekt odpowiedzi przesłany z oddziału regionalnego wymaga podpisu radcy prawnego.
12. Dane osobowe udostępnia się na wniosek sporządzony w wymaganej formie, spełniający warunki formalne i merytoryczne określone w przepisach powszechnie obowiązującego prawa. Wniosek nie spełniający ww. warunków należy rozpatrzyć negatywnie. Szczegółowe zasady postępowania przy rozpatrywaniu wniosków o udostępnienie danych osobowych określa „Instrukcja rozpatrywania wniosków o udostępnienie danych osobowych". Obowiązująca Instrukcja jest opracowywana, aktualizowana i udostępniania w sieci wewnętrznej na stronie intranetowej Agencji przez dyrektora komórki właściwej ds. bezpieczeństwa informacji.
13. Informacje zawierające dane osobowe są udostępniane uprawnionym podmiotom:
    1) w formie pisemnego wydruku, listem poleconym lub za potwierdzeniem osobistego odbioru,
    2) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),

3) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,

4) w inny sposób określony przepisami prawa lub umową.

14. Podstawową formą przekazywania danych osobowych jest metoda określona w ust. 13 pkt 1.

15. W szczególnie uzasadnionych przypadkach stosuje się metody określone w ust. 13 pkt 2–4. Uzasadnienie takiego przypadku, sporządzone na piśmie, dołącza się do akt sprawy.

16. Zawartość elektronicznych nośników informacji podlega kontroli i pisemnej akceptacji bezpośredniego przełożonego - osoby przygotowującej informację określoną w ust. 13.

17. Jeżeli tryb udostępniania danych osobowych określa umowa, przepisów niniejszego rozdziału nie stosuje się w zakresie postanowień umowy.

18. 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.

1a. 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.

2. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy zawartej zgodnie z Ustawą.

3. Umowa powierzenia przetwarzania danych powinna określać co najmniej:

1) zakres i cel przetwarzania danych osobowych,

2) zobowiązanie podmiotu, któremu powierza się dane osobowe do zastosowania odpowiednich środków zabezpieczających te dane,

3) oświadczenie o spełnieniu wymagań, o których mowa w przepisach wykonawczych do Ustawy,

4) postanowienia określające sposób sprawowania przez Agencję kontroli należytego wykonania umowy w powyższym zakresie,

5) postanowienia określające sposób dochodzenia roszczeń Agencji w przypadku, gdy nastąpi naruszenie ochrony danych z przyczyn leżących po stronie podmiotu, któremu powierza się ich przetwarzanie,

6) postanowienia dotyczące wydawania upoważnień do przetwarzania danych osobowych.

3a. Dyrektor komórki właściwej ds. bezpieczeństwa informacji określa wzór umowy powierzenia przetwarzania danych osobowych obowiązujący w Agencji.

4. 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) dyrektora komórki właściwej ds. bezpieczeństwa informacji,

   3) Administratora Systemu.

5. 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) kierownika komórki organizacyjnej przygotowującej projekt,

   2) Inspektora Bezpieczeństwa Informacji w OR,

   3) radcę prawnego.

6. Właściciele zbiorów i dyrektorzy oddziałów regionalnych prowadzą wykaz umów powierzenia przetwarzania danych według wzoru stanowiącego załącznik nr 7 do niniejszego regulaminu.

Rozdział 11
Postępowanie w przypadku kontroli GIODO

§22.

1. GIODO, zastępca GIODO lub upoważnieni przez niego pracownicy Biura GIODO, zwani dalej "inspektorami", mają prawo do przeprowadzania kontroli w Agencji.

2. Inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej komórki lub jednostki organizacyjnej.

3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji jest zawiadamiany bez zbędnej zwłoki o kontroli GIODO w Agencji i może być obecny podczas wykonywania przez inspektorów 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 dyrektorem komórki właściwej ds. bezpieczeństwa informacji, a także z wyznaczonymi przez dyrektora pracownikami tej komórki.

5. Dyrektor komórki właściwej ds. bezpieczeństwa informacji zapewnia pod względem organizacyjnym warunki niezbędne do przeprowadzenia kontroli GIODO w Centrali Agencji.
6. Merytoryczną obsługę kontroli GIODO polegającą m.in. na udzieleniu inspektorom 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) dyrektor komórki właściwej ds. bezpieczeństwa informacji,
   5) *(skreślony),*
   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 GIODO w oddziale regionalnym.
8. Merytoryczną obsługę kontroli GIODO 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. Podczas czynności kontrolnych wykonywanych przez inspektorów GIODO w oddziale regionalnym jest obecny Inspektor Bezpieczeństwa Informacji z OR. Dyrektor oddziału regionalnego może wyznaczyć też inne osoby, które będą uczestniczyły 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.

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w Ustawie oraz w Kodeksie karnym.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Agencji może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością cywilną oraz dyscyplinarną pracowników.

Zmiany wprowadzone - zarządzeniem Nr 31/2015 z dnia 19 maja 2015 r.

Zmiany wprowadzone - zarządzeniem Nr 15/2018 z dnia 26 lutego 2018 r.

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

Załącznik nr 2 do Regulaminu ochrony danych osobowych

.....

.....

.....

.....
(…)*, ***

Oświadczenie

Ja, niżej podpisany(a), oświadczam, iż zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych zobowiązuję się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych zgromadzonych w zasobach ARiMR oraz ich treści, jak również innych danych prawem chronionych. Tajemnicę tę zachowam również po ustaniu okresu wykonywania pracy (lub świadczenia usług) na rzecz ARiMR.

Oświadczam, że zapoznałem(am) się z powszechnie obowiązującymi przepisami o ochronie danych osobowych i wewnętrznymi regulacjami ARiMR dotyczącymi bezpieczeństwa i zasad przetwarzania danych w Agencji, o których mowa w § 15 ust. 3 regulaminu ochrony danych osobowych. Jestem też świadomy(a) odpowiedzialności karnej ustanowionej w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz odpowiedzialności dyscyplinarnej w przypadku naruszenia przepisów o ochronie danych osobowych.

Oświadczam, że uczestniczyłem(am) w szkoleniu z zakresu ochrony danych osobowych**.

....., dn. .....r.
(miejsce i data złożenia oświadczenia)

.....
(czytelny podpis osoby składającej oświadczenie)

* Wypełnić wstawiając: imię i nazwisko, indywidualny numer pracownika nadany w systemie kadrowo-płacowym ARiMR (KIP) i jednostkę organizacyjną, 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 wykonywana jest praca

** Niepotrzebne skreślić

*** Wypełniać drukowanymi literami

Załącznik nr 3 do Regulaminu ochrony danych osobowych

Znak sprawy:

Upoważnienie do przetwarzania danych osobowych poza zbiorami

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r., poz. 1182 ze zm.) upoważniam/odbieram upoważnienie* do przetwarzania danych osobowych

.....
(…)**

w zakresie niezbędnym do wykonywania powierzonej pracy***.

……
(data, pieczątka imienna i podpis dyrektora komórki właściwej ds. kadrowych /dyrektora OR)

* Niepotrzebne skreślić

** Wypełnić wstawiając: imię i nazwisko, indywidualny numer pracownika nadany w systemie kadrowo-płacowym ARiMR (KIP) i jednostkę organizacyjną, w której wykonuje on pracę;
Dla innej osoby niż pracownik – imię i nazwisko, określenie statusu prawnego (np. wolontariusz, stażysta, praktykant, zleceniobiorca itp.) ze wskazaniem komórki i jednostki organizacyjnej ARiMR, w której wykonuje pracę

*** Wynika z zakresu obowiązków pracowniczych lub innej podstawy wykonywania pracy

Załącznik nr 4 do Regulaminu ochrony danych osobowych

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 5 do Regulaminu ochrony danych osobowych

Znak sprawy:

Upoważnienie do przetwarzania danych osobowych w zbiorach przetwarzanych w formie papierowej

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r., poz. 1182 ze zm.) upoważniam/odbieram upoważnienie* do przetwarzania danych osobowych

.....
(imię, nazwisko, stanowisko, komórka organizacyjna)

do przetwarzania danych osobowych w zbiorze .....

.....

.....

w następującym zakresie : .....

.....

.....

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

* Niepotrzebne skreślić

Załącznik nr 6 do Regulaminu ochrony danych osobowych

(usunięty)

Załącznik nr 7 do Regulaminu ochrony danych osobowych

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 .