

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Spis treści:

Rozdział 1 Definicje	2
Rozdział 2 Cel przetwarzania danych osobowych	3
Rozdział 3 Zasada rozliczalności	3
Rozdział 4 Organizacja bezpieczeństwa.....	3
Rozdział 5 Zasada ograniczenia celu przetwarzania	14
Rozdział 6 Zasada ograniczenia przechowywania (retencja danych)	14
Rozdział 7 Prowadzenie dokumentacji w zakresie bezpieczeństwa danych osobowych i instrukcji zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych	16
Rozdział 8 Zasada uwzględniania ochrony danych osobowych w fazie projektowania (Privacy by design) oraz zasada domyślnej ochrony danych (Privacy by default).....	17
Rozdział 9 Ocena skutków dla ochrony danych osobowych (DPIA).....	18
Rozdział 10 Tworzenie i usuwanie zbiorów danych osobowych	20
Rozdział 11 Nadawanie, zmiana i odbieranie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych	22
Rozdział 12 Ewidencja osób upoważnionych do przetwarzania danych osobowych	26
Rozdział 13 Realizacja obowiązku informacyjnego i praw osób, których dane dotyczą.....	26
Rozdział 14 Udostępnianie danych osobowych	28
Rozdział 15 Powierzenie przetwarzania danych osobowych innym podmiotom.....	30
Rozdział 16 Postępowanie w przypadku kontroli PUODO.....	32
Rozdział 17 Odpowiedzialność za naruszenie zasad ochrony danych osobowych	34
Załącznik nr 1 - Wykaz obszarów przetwarzania danych osobowych w ARiMR	35
Załącznik nr 2 - Upoważnienie do przetwarzania danych osobowych.....	36
Załącznik nr 3 - Wykaz osób upoważnionych do przetwarzania danych poza zbiorami	38
Załącznik nr 4 - Upoważnienie do przetwarzania danych osobowych.....	39
Załącznik nr 5 - Rejestr wniosków o realizację praw osób, których dane dotyczą	40
Załącznik nr 6 - Ankieta.....	41
Załącznik nr 7 - Wykaz umów powierzenia przetwarzania danych osobowych.....	48

Rozdział 1

Definicje

§ 1.

Użyte w regulaminie określenia oznaczają:

- 1) Administrator danych – Agencja Restrukturyzacji i Modernizacji Rolnictwa;
- 2) Data Protection Impact Assessment (DPIA) – ocena skutków dla ochrony danych osobowych;
- 3) 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.
- 4) Osoba, której dane dotyczą/Podmiot danych – każda osoba fizyczna, których dane są przetwarzane przez Administratora danych;
- 5) 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;
- 6) Prawa osób, których dane dotyczą – prawa, o których mowa w art. 15-22 RODO;
- 7) Privacy by default – oznacza uwzględnienie ochrony danych osobowych w zakresie podstawowym (domyślne), tj. wdrożenie takich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczy to ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Zastosowane środki powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych;
- 8) Privacy by design – oznacza uwzględnienie ochrony danych osobowych na etapie projektowania systemu służącego do przetwarzania danych osobowych oraz na etapie wykorzystywania go do przetwarzania danych, poprzez zastosowanie odpowiednich środków, o których mowa w art. 25 ust. 1 RODO;
- 9) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
- 10) UODO – Urząd Ochrony Danych Osobowych;
- 11) Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- 12) Właściciel rejestru czynności przetwarzania – Dyrektor komórki organizacyjnej w Centrali Agencji wykonujący czynności przetwarzania i prowadzący rejestr czynności przetwarzania;
- 13) Właściciel zbioru – Dyrektor komórki organizacyjnej w Centrali Agencji, któremu powierzono zbiór danych osobowych;
- 14) Współadministrator – Administrator danych, który wspólnie z innym lub innymi Administratorami danych 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 danych podlegają;

- 15) 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;

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 innych przepisach prawa powszechnie obowiązującego.
2. Dane osobowe są przetwarzane do czasu realizacji celu, dla którego zostały pozyskane, chyba, że obowiązujące przepisy prawa stanowią inaczej.
3. Każda zmiana celu przetwarzania danych osobowych powinna podlegać weryfikacji pod względem zgodności z RODO.
4. 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

Zasada rozliczalności

§ 3.

1. Wszelkie czynności podejmowane w celu realizacji niniejszego regulaminu lub inne czynności podejmowane w zakresie dotyczącym przetwarzania lub ochrony danych osobowych w Agencji, bez względu na formę i sposób ich przetwarzania, winny być dokumentowane przez osoby dokonujące tych czynności, tak, aby Administrator danych mógł wykazać przestrzeganie przepisów RODO.
2. Udokumentowanie, o którym mowa w ust. 1 może nastąpić w dowolnej formie.

Rozdział 4

Organizacja bezpieczeństwa

§ 4.

1. Przestrzeganie zasad ochrony danych osobowych należy do obowiązków osób zatrudnionych, osób wykonujących pracę na rzecz Agencji, osób odbywających praktykę, staż, wolontariat oraz podmiotów gospodarczych i osób fizycznych zewnętrznych współpracujących z Agencją.
2. Administrator danych zapewnia, aby przetwarzanie danych odbywało się zgodnie z prawem. Wdraża odpowiednie środki organizacyjne i techniczne, aby przetwarzanie danych odbywało się zgodnie z prawem oraz aby móc to wykazać.
3. Właściciel zbioru wykonuje obowiązki Administratora danych wobec powierzonego mu zbioru danych osobowych.

4. 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, zabranieniem przez osobę nieuprawnioną, ich zmianą, utratą, uszkodzeniem lub zniszczeniem oraz zapewnić, aby dane były przetwarzane zgodnie z przepisami prawa.
5. Szczegółowe zakresy obowiązków i odpowiedzialności Właściciela Zasobu ustanowione w Polityce bezpieczeństwa informacji w ARiMR stosuje się odpowiednio do Właściciela zbioru.
6. Szczegółowe zakresy obowiązków i odpowiedzialności Właściciela zbioru ustanowione w §7 ust. 2 i 3 stosuje się odpowiednio do Właściciela rejestru czynności przetwarzania.
7. Właściciel zbioru nie może delegować swoich zadań do Podmiotów zewnętrznych.
8. Dyrektor oddziału regionalnego nie jest Właścicielem zbioru.

§ 5.

1. Dyrektor komórki właściwej ds. bezpieczeństwa:
 - 1) określa politykę ochrony danych osobowych oraz dokonuje jej wykładni poprzez:
 - a) określanie zasad ochrony danych osobowych i zarządzania danymi osobowymi;
 - b) określenie jednolitego dla całej Agencji sposobu prowadzenia dokumentacji, o której mowa w przepisach o ochronie danych osobowych oraz dokumentowania wykonania czynności wymaganych tymi przepisami;
 - c) określanie zasad przetwarzania danych osobowych m.in. ich udostępniania i powierzania;
 - d) inicjowanie, tworzenie i aktualizację wewnętrznych aktów normatywnych, procedur oraz innych dokumentów wynikających z zadań powierzonych w polityce ochrony danych osobowych;
 - e) opiniowanie wewnętrznych i zewnętrznych aktów normatywnych, procedur i innych dokumentów wytworzonych w Agencji oraz umów (w tym umów powierzenia przetwarzania danych) i porozumień pod względem zgodności z przepisami o ochronie danych osobowych;
 - 2) określa rozwiązania organizacyjne i systemowe regulujące zasady i sposób zarządzania bezpieczeństwem danych;
 - 3) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa danych;
 - 4) zarządza ryzykiem związanym z przetwarzaniem danych osobowych w celu określenia adekwatnych technicznych i organizacyjnych środków ochrony danych osobowych;
 - 5) nadzoruje działania związane z wykrytymi incydentami;
 - 6) zapewnia w porozumieniu z IOD działania audytowe w zakresie przestrzegania zasad określonych w niniejszym regulaminie;
 - 7) określa Dyrektorom komórek i jednostek organizacyjnych Agencji zadania mające na celu zapewnienie bezpieczeństwa danych, w przypadku wystąpienia takiej potrzeby;

- 8) wspiera Inspektora Ochrony Danych w realizacji jego zadań i zapewnia niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych;
- 9) reprezentuje Administratora danych w postępowaniach skargowych prowadzonych przed PUODO.

§ 6.

1. Do zadań Inspektora Ochrony Danych należy:

- 1) informowanie Administratora danych, podmiotu przetwarzającego oraz osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisach o ochronie danych osobowych;
- 2) doradzanie Administratorowi danych, podmiotowi przetwarzającemu oraz osobom, które przetwarzają dane w sprawie obowiązków z zakresu ochrony danych osobowych;
- 3) monitorowanie przestrzegania RODO i innych przepisów o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych. Monitorowanie może dotyczyć w szczególności:
 - a) przestrzegania każdej z zasad przetwarzania danych osobowych wynikających z art. 5 RODO, w tym zasady rozliczalności;
 - b) dopuszczalności przetwarzania danych zwykłych na podstawie art. 6 RODO z uwzględnieniem każdej z przesłanek;
 - c) dopuszczalności przetwarzania danych szczególnych kategorii z uwzględnieniem każdej z przesłanek;
 - d) prawidłowości pozyskiwania zgód na przetwarzanie danych osobowych oraz prawidłowości przetwarzania danych na tej podstawie;
 - e) realizacji każdego z praw osób, których dane dotyczą, a także innych praw wynikających z RODO;
 - f) prawidłowości spełnienia obowiązku informacyjnego wobec osób, których dane dotyczą;
 - g) zabezpieczeń organizacyjnych i technicznych danych osobowych, organizacji ich przetwarzania, procesów przetwarzania;
 - h) prawidłowości udostępniania danych osobowych;
 - i) prawidłowości prowadzenia rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania;
 - j) prawidłowości prowadzenia wykazu umów powierzenia przetwarzania danych osobowych;
- 4) podział obowiązków w zakresie monitorowania przestrzegania przepisów o ochronie danych osobowych;
- 5) zwiększanie świadomości personelu uczestniczącego w operacjach przetwarzania danych osobowych, poprzez inicjowanie lub prowadzenie szkoleń (z wyjątkiem szkoleń podstawowych dla osób nowozatrudnionych);
- 6) wykonywanie audytów weryfikujących zgodność przetwarzania danych i sposób przestrzegania obowiązujących w Agencji standardów ochrony danych osobowych we wszystkich komórkach i jednostkach organizacyjnych Agencji oraz rekomendowanie określonych działań w tym zakresie;

- 7) udzielanie na żądanie Właściciela procesu zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 RODO. Dokonując oceny Właściciel procesu 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);
- 8) współpraca z PUODO (organem nadzorczym) w kwestiach związanych z przetwarzaniem danych osobowych;
- 9) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz – w stosownych przypadkach – prowadzenie konsultacji we wszelkich innych sprawach;
- 10) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą;
- 11) dokonywanie oceny, czy istnieje w danym stanie faktycznym wymóg zgłaszania naruszenia ochrony danych osobowych;
- 12) dokonywanie oceny, czy istnieje w danym stanie faktycznym wymóg zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych;
- 13) prowadzenie rejestru naruszeń ochrony danych osobowych;
- 14) wspieranie Dyrektora komórki właściwej 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 default);
- 15) wspieranie Dyrektora komórki właściwej ds. bezpieczeństwa w szczególności poprzez:
 - a) rekomendowanie co do rozwiązań związanych z przetwarzaniem danych osobowych;
 - b) inicjowanie tworzenia i aktualizacji dokumentów wynikających z zadań powierzonych w polityce ochrony danych osobowych;
 - c) sporządzanie i przedstawianie stanowiska w sprawie zgodnego z prawem przetwarzania danych osobowych;
 - d) opiniowanie i doradzanie w sprawach dotyczących bezpośrednio lub pośrednio ochrony danych osobowych;
 - e) opiniowanie rozwiązań organizacyjnych pod kątem właściwego wdrażania systemu ochrony danych osobowych.

2. Wykonując swoje obowiązki Inspektor Danych Osobowych może w szczególności:

- 1) żądać wyjaśnień i informacji od Właścicieli zbiorów, Właścicieli rejestru czynności przetwarzania, Dyrektorów oddziałów regionalnych, jak również od wszystkich pracowników i osób przetwarzających dane pozyskiwane przez Administratora danych, w celu identyfikacji procesów i sprawdzenia zgodności przetwarzania danych osobowych z prawem;
 - 2) wydawać zalecenia Właścicielom zbiorów, Właścicielom rejestru czynności przetwarzania, Dyrektorom oddziałów regionalnych i innym osobom odpowiedzialnym za ochronę i zgodne z prawem przetwarzanie danych osobowych w Agencji, dotyczące sposobu przetwarzania danych osobowych i zgodnego z prawem ich przetwarzania;
 - 3) wyznaczać Właścicielom zbiorów, Właścicielom rejestru czynności przetwarzania, Dyrektorom oddziałów regionalnych obowiązki co do sposobu stosowania i przestrzegania RODO oraz innych aktów prawnych w zakresie ochrony danych osobowych, jak również wewnętrznych uregulowań dotyczących przetwarzania danych osobowych w Agencji.
3. Właściciele zbiorów, Właściciele rejestru czynności przetwarzania, Dyrektorzy oddziałów regionalnych oraz osoby przetwarzające dane osobowe zatrudnione w ARiMR na podstawie umowy o pracę oraz osoby wykonujące pracę na rzecz ARiMR, a także stażyści, praktykanci i wolontariusze oraz podmioty gospodarcze i osoby fizyczne zewnętrzne współpracujące z ARiMR 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 osobowych. Osoby te zobowiązane są do udzielenia wyjaśnień i informacji w terminie wskazanym przez Inspektora Ochrony Danych, w tym wykonywania poleceń Inspektora Ochrony Danych w powyższym zakresie.

§ 7.

1. Każdy zbiór danych osobowych przetwarzanych w Agencji posiada Właściciela zbioru, którego ustala Prezes ARiMR w zarządzeniu.
2. Właściciel zbioru odpowiada za realizację 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 zapewnić, aby te dane zostały usunięte albo zanonimizowane;
- 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 przekazania, 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) Właściciel zbioru jest zobowiązany do:
 - a) weryfikowania na bieżąco zgodności faktycznego przetwarzania z opisem procesu, zawartym w rejestrze czynności przetwarzania, w szczególności:
 - celów przetwarzania danych;
 - podstawy prawnej przetwarzania danych;
 - zakresu przetwarzanych danych;

- spełnienia obowiązku informacyjnego;
 - pozyskania zgód na przetwarzanie danych – o ile dotyczy;
- b) nieprzetwarzania danych osobowych w ramach procesów nie wpisanych do rejestru czynności;
- 4) zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane i/lub udostępniane m.in. prowadzenie ewidencji udostępnień danych osobowych w systemie teleinformatycznym;
 - 5) nadawanie upoważnień do przetwarzania danych osobowych;
 - 6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
 - 7) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną w oparciu o szacowanie ryzyka;
 - 8) nadzorowanie systemów teleinformatycznych służących do przetwarzania danych osobowych za pośrednictwem Administratora Systemu;
 - 9) terminowe przekazywanie Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych – informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;
 - 10) zapewnienie warunków i pomocy osobom dokonującym kontroli, o której mowa w § 29 ust. 1;
 - 11) 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;
 - 12) obsługę wniosków osób, których dane dotyczą związanych z realizacją ich praw, w zakresie przetwarzania ich danych osobowych;
 - 13) prowadzenie rejestru wniosków osób, których dane dotyczą, związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych;
 - 14) w przypadku złożenia do PUODO skargi na przetwarzanie danych osobowych przez Administratora danych - przekazanie w terminie wskazanym przez Dyrektora komórki właściwej ds. bezpieczeństwa: pełnej dokumentacji sprawy, której dotyczy skarga, odpowiedzi na pytania PUODO, wyjaśnień, stanowiska co do zarzutów zawartych w skardze oraz innych informacji niezbędnych w sprawie; za terminowość, kompletność i prawidłowość przekazanej informacji odpowiedzialność ponosi Właściciel zbioru;
 - 15) wyznaczenie co najmniej dwóch osób do spraw z zakresu ochrony danych osobowych, w tym w szczególności do: realizacji obowiązku informacyjnego, udostępniania danych osobowych, rozpatrywania wniosków o realizację praw osób, których dane dotyczą;
 - 16) wykonywanie poleceń, zaleceń i rekomendacji Dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych dotyczących ochrony i przetwarzania danych osobowych;
 - 17) zapewnienie uczestnictwa podległych pracowników w szkoleniach dotyczących 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 przetwarzanych 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 przekazania, 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.

§ 8.

1. Administrator Systemu jest odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych w systemie teleinformatycznym oraz za właściwe utrzymanie i funkcjonowanie systemów teleinformatycznych służących do przetwarzania danych osobowych.
2. Administrator Systemu zapewnia, aby każdy system, aplikacja czy proces domyślnie zapewniał najwyższą, wynikającą z analizy ryzyka oceny środków służących bezpieczeństwu, ochronę danych osobowych oraz żeby zmniejszenie ochrony było możliwe jedynie na wyraźne żądanie Właściciela zasobu i tylko w uzasadnionych przypadkach.
3. Administrator Systemu:
 - 1) jest odpowiedzialny za realizację domyślnej ochrony danych osobowych oraz za ochronę danych osobowych w fazie projektowania;
 - 2) jest zobowiązany, w zakresie swoich kompetencji, do zgłaszania Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych każdej planowanej zmiany środków technicznych lub organizacyjnych stosowanych w sieciach lub systemach teleinformatycznych, w których są przetwarzane dane osobowe;
 - 3) jest zobowiązany, w zakresie swoich kompetencji, do zgłaszania Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych każdej planowanej modyfikacji funkcjonalności systemów teleinformatycznych, w których są lub będą przetwarzane dane osobowe, mającej lub mogącej mieć wpływ na zakres lub sposób przetwarzania danych osobowych;
 - 4) jest zobowiązany do zgłaszania Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych każdego planowanego zakupu sprzętu teleinformatycznego, systemu teleinformatycznego lub planowanego zawarcia umowy na dostarczanie usług przez Podmiot zewnętrzny;
 - 5) bierze udział w przeprowadzaniu oceny skutków dla ochrony danych i oceny ryzyka w ramach oceny środków służących ich bezpieczeństwu;
 - 6) jest odpowiedzialny za opracowanie procedury sposobu usuwania danych z systemów teleinformatycznych;

- 7) bierze udział w procedowaniu dotyczącym incydentów bezpieczeństwa danych;
 - 8) bierze udział w przygotowywaniu odpowiedzi na wnioski osób, których dane osobowe dotyczą, w zakresie realizacji ich praw z RODO;
 - 9) odpowiada za realizację praw osób, których dane osobowe dotyczą, w zakresie, w jakim dotyczą one przetwarzania danych osobowych w formie elektronicznej;
 - 10) jest zobowiązany do udzielania Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych wszelkich informacji niezbędnych do realizacji ich zadań.
4. Administrator Systemu odpowiada za usunięcie danych z systemu teleinformatycznego w momencie zaprzestania przetwarzania danych osobowych.

§ 9

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 § 7 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) załatwiania wniosków o udostępnienie danych;
 - 3) zawierania umów powierzenia przetwarzania danych realizowanych w oddziale regionalnym;
 - 4) terminowego przekazywania Dyrektorowi komórki właściwej ds. bezpieczeństwa informacji oraz Inspektorowi Ochrony Danych - informacji i wyjaśnień niezbędnych do wykonywania wyznaczonych im zadań;
 - 5) zapewnienia warunków i pomocy osobom dokonującym audytu w oddziale regionalnym i podległych biurach powiatowych;
 - 6) obsługi wniosków osób, których dane dotyczą związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych;
 - 7) prowadzenie rejestru wniosków osób, których dane dotyczą, związanych z realizacją ich praw w zakresie przetwarzania ich danych osobowych;
 - 8) w przypadku złożenia do PUODO skargi na przetwarzanie danych osobowych przez Administratora danych - przekazanie w terminie wskazanym przez Dyrektora komórki właściwej ds. bezpieczeństwa: pełnej dokumentacji sprawy, której dotyczy skarga, odpowiedzi na pytania PUODO, wyjaśnień, stanowiska co do zarzutów zawartych w skardze oraz innych informacji niezbędnych w sprawie; za terminowość, kompletność i prawidłowość przekazanej informacji odpowiedzialność ponosi Dyrektor oddziału regionalnego;
 - 9) wykonywanie poleceń, zaleceń i rekomendacji Dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych dotyczących ochrony i przetwarzania danych osobowych;
 - 10) zapewnienie uczestnictwa podległych pracowników w szkoleniach dotyczących danych osobowych;

- 11) wyznaczenia co najmniej dwóch osób do spraw z zakresu ochrony danych osobowych, w tym w szczególności do: realizacji obowiązku informacyjnego, udostępniania danych osobowych, rozpatrywania wniosków o realizację praw osób, których dane dotyczą.

§ 10.

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) prowadzenie, 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 § 22 ust. 3, przeprowadzonych m.in. dla kierowników biur powiatowych, zawierających m.in. prezentację na szkolenie i listy obecności uczestników oraz komunikatów i innych czynności, o których mowa w § 22 ust. 4;
- 6) w przypadku złożenia do PUODO skargi na przetwarzanie danych osobowych przez Administratora danych – przygotowanie pełnej dokumentacji sprawy, której dotyczy skarga, odpowiedzi na pytania PUODO, wyjaśnień, stanowiska co do zarzutów zawartych w skardze oraz innych informacji niezbędnych w sprawie oraz bezpośrednia współpraca w tym zakresie z Dyrektorem komórki właściwej ds. bezpieczeństwa lub osobą przez niego wskazaną.

§ 11.

1. Dyrektor komórki właściwej 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, Właścicielom rejestru czynności przetwarzania, 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 default);

- 3) audytowania sposobu przetwarzania danych osobowych i przestrzegania obowiązujących standardów ich ochrony w odniesieniu do zastosowanych środków technicznych i organizacyjnych w Agencji;
 - 4) prowadzenia szkoleń dotyczących przestrzegania polityki ochrony danych osobowych w Agencji;
 - 5) wspierania Inspektora Ochrony Danych w realizacji jego zadań.
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 czynności audytowych w zakresie przetwarzania danych osobowych w oddziale regionalnym i w biurach powiatowych;
 - 2) prowadzenia czynności audytowych w zakresie przestrzegania w oddziale regionalnym i w 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) opiniowania nowych projektów pod kątem zgodności z zasadami ochrony w fazie projektowania oraz domyślnej ochrony danych (Privacy by design, Privacy by default).
5. Dyrektor komórki właściwej 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 audytów/czynności audytowych Inspektorom Bezpieczeństwa Informacji w Centrali/oddziale regionalnym wydaje odpowiednio:
- 1) Prezes ARiMR;
 - 2) Dyrektor oddziału regionalnego.

§ 12.

1. Właściciel zbioru, Właściciel rejestru czynności przetwarzania oraz Dyrektor oddziału regionalnego mogą występować do Dyrektora komórki właściwej ds. bezpieczeństwa lub Inspektora Ochrony Danych o stanowisko w sprawach związanych z ochroną i przetwarzaniem danych osobowych, mieszczących się w zakresie realizacji zadań wnioskodawcy.
2. Wniosek o stanowisko powinien zawierać dokładny opis stanu faktycznego i stanu prawnego, ze wskazaniem konkretnych przepisów prawa mających zastosowanie w danej sprawie, precyzyjne pytanie w kwestiach budzących wątpliwości oraz stanowisko wnioskodawcy w tym zakresie. Do wniosku należy dołączyć wszystkie dokumenty i materiały niezbędne do zajęcia stanowiska.
3. W sprawach, w których podobny stan faktyczny był już przedmiotem wniosku, o którym mowa w ust. 2 i nie uległ on zmianie, podobnie zmianie nie uległ stan prawny, Dyrektor komórki właściwej ds. bezpieczeństwa lub Inspektor Ochrony Danych ma prawo

odmówić zajęcia kolejnego stanowiska i odesłać do wcześniejszego rozstrzygnięcia w tej sprawie.

Rozdział 5

Zasada ograniczenia celu przetwarzania

§13.

1. Właściciele zbiorów dbają o to, aby dane osobowe były przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach, określonych w momencie ich zbierania. Niedopuszczalne jest zbieranie danych osobowych „na zapas”, dla przyszłych, nieznaczonych jeszcze celów.
2. Przetwarzanie danych w innym celu niż cel pierwotny, jest możliwe tylko w sytuacji, kiedy zmiana celu ma uzasadnienie i podstawy prawne, a także kiedy zostanie przeprowadzona ocena ryzyka naruszenia praw lub wolności osób fizycznych, której wynik będzie na poziomie niskim oraz kiedy zostanie zrealizowany obowiązek informacyjny przed dalszym przetwarzaniem. Obowiązek informacyjny nie musi być realizowany, jeśli istnieją przesłanki zwalniające z tego obowiązku.
3. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami przetwarzania.

Rozdział 6

Zasada ograniczenia przechowywania (retencja danych)

§ 14.

1. Właściciel zbioru zapewnia, że dane osobowe są przechowywane z uwzględnieniem zasady ograniczenia przechowywania, tj. w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane – dane osobowe przetwarzane są tak długo, jak długo jest to uzasadnione oraz zgodne z przepisami prawa (okres retencji danych), z zastrzeżeniem ust. 2.
2. W przypadkach, gdy okresy retencji danych osobowych nie wynikają wyraźnie z przepisów prawa, Właściciel zbioru określa te okresy samodzielnie.
3. Właściciel zbioru zapewnia, że w przypadku dezaktualizacji wszystkich celów przetwarzania danych osobowych nie są realizowane jakiegokolwiek operacje na tych danych z wyjątkiem ich usunięcia. Przez usunięcie danych należy również rozumieć nieodwracalną anonimizację danych.
4. Zgodnie z wymaganiami RODO dla każdego rozpoznanego procesu przetwarzania danych osobowych (czynności przetwarzania) należy określać okres, przez który dane osobowe, przetwarzane w ramach tego procesu, będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.
5. Kryteria ustalania okresu, o których mowa w ust. 4 mogą być określone w poniższy sposób:

- 1) przez okres wymagany przepisami prawa;
 - 2) do czasu zakończenia realizacji umowy i związanych z nią roszczeń;
 - 3) do czasu cofnięcia zgody lub zgłoszenia sprzeciwu.
6. Określając okresy retencji uwzględnia się w szczególności:
- 1) obowiązki prawne ciążące na Administratorze danych w zakresie przechowywania określonych danych osobowych lub dokumentów zawierających dane osobowe, wynikające z przepisów prawa;
 - 2) potencjalną niezbędność przetwarzania danych dla celów związanych z ustalaniem lub dochodzeniem roszczeń oraz obroną przed takimi roszczeniami i związane z tym okresy przedawnienia roszczeń wynikające z Kodeksu cywilnego lub przepisów innych ustaw.
- Okresy retencji mogą ulegać zmianie w związku ze zmianą obowiązujących przepisów prawa mających wpływ na okres retencji danych.
7. Przed usunięciem danych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, w szczególności poprzez sprawdzenie czy:
- 1) nie występuje obowiązek prawny ciążący na Administratorze danych, którego wykonanie wymaga przetwarzania danych osobowych;
 - 2) nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, zgodnie z właściwymi przepisami, skutkujące koniecznością dalszego przetwarzania danych osobowych.
8. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji, w przypadku, gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych - na zasadach określonych w art. 89 ust. 1 RODO - pod warunkiem, że wdrożone są odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.
9. Właściciel zbioru weryfikuje dane osobowe przetwarzane w celu realizacji ustawowych zadań realizowanych przez niego, nie rzadziej niż co 5 lat od dnia ich uzyskania. Dane zbędne Właściciel zbioru usuwa.
10. W razie wątpliwości, przed usunięciem danych osobowych Właściciel zbioru zasięga opinii Inspektora Ochrony Danych.
11. Właściciel zbioru podejmuje działania w celu usunięcia danych osobowych w systemie teleinformatycznym i poza nim oraz ze wszystkich nośników.
12. Właściciel zbioru przekazuje Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych informację o usuniętych danych osobowych zawierającą:
- 1) nazwę zbioru, z którego usuwane są dane osobowe;
 - 2) podstawę prawną usunięcia danych osobowych;
 - 3) opis usuniętych danych, np. wskazanie, że usunięto dane osobowe zwykle w postaci imienia i nazwiska, numeru identyfikacyjnego (np. PESEL, NIP, nr producenta rolnego), danych adresowych;

- 4) opis sposobu usunięcia danych osobowych;
- 5) wskazanie z jakich nośników zostały usunięte dane osobowe, np. czy z dokumentów, czy z systemu teleinformatycznego;
- 6) datę usunięcia danych;
- 7) miejsce i datę sporządzenia informacji;
- 8) podpis Właściciela zbioru danych.

Rozdział 7

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

§ 15.

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 właściwej 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 właściwej 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, przy czym środki te nie mogą być niższe niż ustalone dla domyślnej ochrony, zgodnie z zasadami określonymi w Regulaminie eksploatacji systemów teleinformatycznych (ICT).
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 oraz Inspektorowi Ochrony Danych.

§ 16.

1. Dokument „Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych”, wskazuje dokumenty, które określają sposoby realizacji wymogów dotyczących ochrony danych osobowych.
2. Instrukcję zarządzania systemem teleinformatycznym 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 teleinformatycznym 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 8

Zasada uwzględniania ochrony danych osobowych w fazie projektowania (Privacy by design) oraz zasada domyślnej ochrony danych (Privacy by default)

§ 17.

1. We wszelkich działaniach zmierzających do przetwarzania danych osobowych, począwszy od etapu planowania, Właściciel zbioru uwzględnia konieczność zapewnienia ich ochrony, biorąc pod uwagę:
 - 1) stan wiedzy technicznej;
 - 2) koszt wdrożenia zabezpieczeń;
 - 3) charakter, zakres, kontekst i cele przetwarzania;
 - 4) ryzyko naruszenia praw lub wolności osób fizycznych.
2. Przy tworzeniu lub modyfikacji systemów teleinformatycznych służących do przetwarzania danych osobowych, a także innych rozwiązań wspierających czynności przetwarzania danych osobowych, Właściciel zbioru/Dyrektor komórki właściwej ds. informatyki odpowiada za uwzględnienie ochrony danych osobowych - od fazy koncepcyjnej - zarówno w architekturze systemu, jak i w procesach biznesowych, które są przez ten system obsługiwane.
3. Środki służące realizacji zasady uwzględniania ochrony danych osobowych w fazie projektowania polegają między innymi na:
 - 1) minimalizacji zakresu przetwarzanych danych osobowych;
 - 2) minimalizacji okresu przetwarzania danych osobowych;
 - 3) pseudonimizacji danych osobowych;
 - 4) umożliwieniu zapewnienia realizacji praw osób, których dane dotyczą;

- 5) zaplanowaniu i wdrożeniu zabezpieczeń w celu spełnienia zasad ochrony danych osobowych, określonych w niniejszym regulaminie.
4. Właściciel zbioru danych/Dyrektor komórki właściwej ds. informatyki realizuje zasadę Privacy by design na etapie przygotowywania dokumentacji we wszystkich zamówieniach publicznych, które przewidują przetwarzanie danych osobowych.
5. Przed wdrożeniem nowego procesu przetwarzania danych osobowych należy również rozważyć przeprowadzenie oceny skutków dla ochrony danych.
6. Wdrożenie odpowiednich środków technicznych i organizacyjnych dla ochrony przetwarzanych w procesie danych osobowych winno być dokonane w taki sposób, aby wszelkie działania w tym zakresie były odpowiednio udokumentowane, na potrzeby realizacji zasady rozliczalności.
7. Właściciel zbioru stosuje zasadę domyślnej ochrony danych, która polega na tym, że dopuszczalne jest przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania (zasada minimalizacji danych). Obowiązek ten odnosi się do zakresu zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

Rozdział 9

Ocena skutków dla ochrony danych osobowych (DPIA)

§ 18.

1. Celem oceny skutków dla ochrony danych (DPIA) jest zapewnienie przez Administratora danych przestrzegania przepisów RODO oraz właściwego zarządzania ryzykiem, a w szczególności, mając na względzie zasadę rozliczalności, umożliwienie wykazania przestrzegania tych przepisów, przy uwzględnieniu m.in. ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i różnej wadze zagrożenia.
2. Ocenę skutków dla ochrony danych wykonuje się dla:
 - 1) jednej operacji przetwarzania, np. dla jednej aplikacji, projektu;
 - 2) wielu operacji przetwarzania, które są podobne pod względem charakteru, zakresu, kontekstu, celu i ryzyka, np. jeżeli operacja przetwarzania jest taka sama u wielu Administratorów, gdy dochodzi do współadministrowania.
3. Przedmiotem oceny skutków dla ochrony danych są:
 - 1) procesy przetwarzania danych osobowych zidentyfikowane w rejestrze czynności przetwarzania;
 - 2) nowe projekty, na etapie projektowania, jeśli podlegają one wymogowi przeprowadzenia oceny.
4. Dokonując oceny skutków należy uwzględnić następujące czynniki:
 - 1) rodzaj przetwarzania, w szczególności przetwarzanie z wykorzystaniem nowych technologii;
 - 2) charakter, zakres, kontekst i cele przetwarzania;

- 3) duże prawdopodobieństwo spowodowania wysokiego naruszenia praw lub wolności osób fizycznych;
 - 4) planowane operacje przetwarzania;
 - 5) przetwarzanie polegające na systematycznej, kompleksowej ocenie czynników osobowych odnoszących się do osób fizycznych, opartej na zautomatyzowanym przetwarzaniu, w tym profilowaniu, będącej podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
 - 6) przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO;
 - 7) przetwarzanie polegające na systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie;
 - 8) czy konkretna operacja lub operacje przetwarzania podlegają obowiązkowej ocenie skutków zgodnie z wykazem ustanowionym przez PUODO;
 - 9) czy konkretna operacja lub operacje przetwarzania podlegają wyłączeniu spod DPIA, zgodnie z wykazem rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych ustanowionej przez PUODO;
 - 10) czy przetwarzanie odbywające się na podstawie art. 6 ust. 1 lit. c lub lit. e RODO ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega Administrator i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej, chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.
5. Ocena skutków dla ochrony danych przeprowadzana jest w przypadku, jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą. Oceny skutków dla ochrony danych dokonuje przed rozpoczęciem przetwarzania (na etapie projektowania), w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi dla ryzyka ochrony danych.
6. Ocena skutków dla ochrony danych składa się z następujących elementów:
- 1) szczegółowego usystematyzowanego opisu planowanych operacji i celów przetwarzania oraz – o ile ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora, oraz środków zabezpieczenia danych;
 - 2) oceny, jakie środki (organizacyjne oraz techniczne) są niezbędne oraz proporcjonalne dla zapewnienia odpowiedniego stopnia ochrony danych osobowych, w szczególności w celu zapewnienia realizacji podstawowych zasad przetwarzania danych oraz zachowania praw osób, których dane dotyczą;

- 3) szczegółowej oceny stopnia ryzyka wynikającego z przetwarzania danych osobowych w nowym projekcie lub procesie oraz doboru adekwatnych środków (organizacyjnych, fizycznych i technicznych) mających na celu ograniczenie ryzyka.
1. Ocena DPIA przeprowadzana jest przez Właściciela zbioru/Dyrektora oddziału regionalnego we współpracy, w razie potrzeby, z Inspektorem Ochrony Danych lub inną wyznaczoną osobą oraz osobą odpowiedzialną za dany proces lub z inicjatorem nowego projektu, a także przy wsparciu komórki ds. prawnych w zakresie problemów prawnych innych niż związane z przepisami o ochronie danych osobowych.

Rozdział 10

Tworzenie i usuwanie zbiorów danych osobowych

§ 19.

1. Dyrektor komórki organizacyjnej w Centrali/Właściciel zbioru zobowiązany jest zawiadomić Dyrektora komórki właściwej 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 przekazania, 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 właściwej 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.

§ 20.

1. W przypadku zaprzestania przetwarzania danych w zbiorze Właściciel zbioru jest zobowiązany niezwłocznie poinformować Dyrektora komórki właściwej 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 danych osobowych ze zbioru danych lub całego zbioru danych osobowych. O tym fakcie informuje Dyrektora komórki właściwej ds. bezpieczeństwa oraz Inspektora Ochrony Danych. W razie wątpliwości, przed usunięciem danych osobowych ze zbioru danych lub całego zbioru danych osobowych Właściciel zbioru zasięga opinii Inspektora Ochrony Danych.
3. Właściciel zbioru podejmuje działania w celu usunięcia danych osobowych ze zbioru danych lub całego zbioru danych osobowych ze wszystkich nośników.
4. Zbiory danych osobowych oraz dane osobowe ze zbiorów danych osobowych są likwidowane komisyjnie.
5. W skład komisji powołanej przez Administratora danych wchodzi:
 - 1) osoba wyznaczona przez Administratora Systemu, jeżeli zbiór jest przetwarzany w systemie teleinformatycznym;
 - 2) dwie osoby reprezentujące Właściciela zbioru.
6. Właściciel zbioru przekazuje Dyrektorowi komórki właściwej ds. bezpieczeństwa oraz Inspektorowi Ochrony Danych kopię protokołu komisyjnie zlikwidowanego zbioru.
7. Protokół, o którym mowa w ust. 6 zawiera:
 - 1) nazwę usuwanego zbioru danych osobowych/nazwę zbioru, z którego usuwane są dane osobowe;
 - 2) podstawę prawną usunięcia zbioru danych osobowych/usunięcia danych osobowych;
 - 3) opis usuniętych danych, np. wskazanie, że usunięto dane osobowe zwykle w postaci imienia i nazwiska, numeru identyfikacyjnego (np. PESEL, NIP, nr producenta rolnego), danych adresowych;
 - 4) opis sposobu usunięcia zbioru danych osobowych/danych osobowych;
 - 5) wskazanie z jakich nośników został usunięty zbiór danych osobowych/dane osobowe, np. czy z dokumentów papierowych, czy z systemu teleinformatycznego;
 - 6) datę i miejsce sporządzenia protokołu usunięcia zbioru danych osobowych/danych osobowych;
 - 7) skład komisji;
 - 8) podpisy członków komisji.

Rozdział 11

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

§ 21.

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

§ 22.

1. Upoważnienie do przetwarzania danych osobowych poza zbiorami (upoważnienie ogólne) może być nadane:
 - 1) osobom przyjmowanym do pracy lub wykonującym zadania na rzecz ARiMR po odbyciu szkolenia podstawowego;
 - 2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania upoważnienia.
2. Inspektor Ochrony Danych publikuje w sieci wewnętrznej na stronie internetowej Agencji, w zakładce Ochrona Danych Osobowych, wykaz aktów prawnych zawierających przepisy o ochronie danych osobowych.
3. 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 bezpieczeństwa informacji, w tym ochrony danych osobowych. 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.
4. Inspektor Bezpieczeństwa Informacji w OR jest zobowiązany w sposób ciągły do podnoszenia świadomości pracowników oddziału regionalnego oraz podległych biur powiatowych w przedmiocie naruszeń ochrony danych osobowych, w szczególności poprzez: wystosowywanie cyklicznych komunikatów przypominających po powtarzających się naruszeniach ochrony danych.
5. Kierujący komórką/jednostką organizacyjną w razie potrzeby wyznacza osoby na szkolenie w zakresie przetwarzania szczególnych kategorii danych osobowych. Obowiązkowemu szkoleniu w zakresie przetwarzania szczególnych kategorii danych podlegają m.in.: członkowie Komisji ds. Gospodarowania Zakładowym Funduszem Świadczeń Socjalnych, członkowie Komisji bezpieczeństwa i higieny pracy oraz Komisji ds. przeciwdziałania mobbingowi i dyskryminacji w ARiMR. Szkolenie prowadzi Inspektor Bezpieczeństwa Informacji odpowiedni dla jednostki organizacyjnej ARiMR, po uprzednim uzgodnieniu terminu szkolenia.
6. 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. 3, przed skierowaniem na szkolenie zapoznają osoby przyjmowane do pracy z aktami prawnymi zawierającymi przepisy o ochronie danych osobowych.

7. Szkoleniu, o którym mowa w ust. 3 podlegają również osoby zatrudnione, a niewykonujące pracy w Agencji przez okres co najmniej 12 miesięcy.
8. Szkoleniu, o którym mowa w ust. 3 nie podlegają osoby, które zmieniają stanowisko w wyniku awansu.
9. 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).
10. Dyrektor komórki właściwej ds. bezpieczeństwa 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 w zakresie bezpieczeństwa informacji oraz szkoleniu w zakresie przetwarzania szczególnych kategorii danych osobowych. Zawiadomienie następuje poprzez wysłanie informacji za pośrednictwem poczty elektronicznej. Osoby, które nie odbyły szkolenia podstawowego oraz w razie potrzeby szkolenia w zakresie przetwarzania szczególnych kategorii danych osobowych, nie mogą zostać dopuszczone do pracy związanej z przetwarzaniem danych osobowych.
11. 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.
12. Treść oświadczenia zamieszczona jest na druku stanowiącym załącznik nr 2 do niniejszego regulaminu. Dokument po wypełnieniu przechowywany jest przez komórkę ds. kadrowych.
13. Kopie list obecności uczestników szkoleń podstawowych przeprowadzanych przez kierowników biur powiatowych oraz oryginały dokumentów zawierających upoważnienie do przetwarzania danych osobowych 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 upoważnienie do przetwarzania danych osobowych 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.
14. Listy obecności ze szkolenia z zakresu szczególnych kategorii danych osobowych przechowuje Inspektor Bezpieczeństwa Informacji właściwy dla danej jednostki organizacyjnej Agencji.
15. 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. Upoważnienia przechowywane są przez komórkę właściwą ds. kadrowych.

16. W szczególnie uzasadnionych przypadkach, Dyrektor komórki właściwej ds. kadrowych w Centrali/Dyrektor oddziału regionalnego mogą nadać upoważnienie osobom wskazanym w ust. 1 bez ich przeszkolenia, równocześnie wskazując obowiązek odbycia ww. szkolenia w terminie nie przekraczającym jednego miesiąca od nadania upoważnienia.
17. 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.
18. 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;
 - 3) Inspektor Ochrony Danych;
 - 4) Dyrektor komórki właściwej ds. bezpieczeństwa.
19. Osoby, o których mowa w ust. 16, podpisują oświadczenie na druku upoważnienia, którego wzór stanowi załącznik nr 2 do niniejszego regulaminu, przekazany przez Dyrektora komórki właściwej ds. kadrowych, w którym zobowiązują się do zachowania w tajemnicy/poufności przetwarzanych danych oraz zastosowanych w Agencji środków ich ochrony.
20. Oświadczenie, o którym mowa w ust. 19 przechowywane jest w ich aktach osobowych.

§ 23.

1. Upoważnienie do przetwarzania danych w zbiorach (upoważnienie szczególne) może być nadane:
 - 1) osobom, które uzyskały upoważnienie ogólne do przetwarzania danych;
 - 2) innym osobom, jeżeli przepisy tak stanowią lub jeżeli zachodzi uzasadniona potrzeba nadania takiego upoważnienia; osobom tym można nadać upoważnienie bez obowiązku uprzedniego uzyskania upoważnienia ogólnego.
2. Upoważnienie do przetwarzania danych w zbiorach przetwarzanych w systemie teleinformatycznym jest nadawane w wyniku zaakceptowania przez Właściciela zbioru wniosku o nadanie uprawnień do pracy w systemie. Druk wniosku określono w Księżce procedur KP-611-101-ARiMR „Obsługa kont użytkowników systemów teleinformatycznych ARiMR”.
3. Wobec zbiorów przetwarzanych w systemie teleinformatycznym 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 teleinformatycznym, przechowywany przez Administratora Systemu, jest częścią ewidencji osób upoważnionych.
7. Wobec zbiorów przetwarzanych w systemie teleinformatycznym w oddziałach regionalnych i biurach powiatowych Agencji wniosek o nadanie uprawnień do pracy w systemie, w imieniu 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 lub w dokumentacji osób wykonujących zadania na rzecz ARiMR.
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. 11, stosuje się odpowiednio zasady kompetencyjne obowiązujące przy sporządzaniu wniosku o nadanie uprawnień do przetwarzania danych w systemie teleinformatycznym.
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.

§ 24.

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 12

Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 25.

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, Zastępcy Prezesa, Inspektor Ochrony Danych oraz Dyrektor komórki właściwej ds. bezpieczeństwa;
 - 2) zbiór osób, które uzyskały upoważnienia do przetwarzania danych w zbiorach:
 - a) przetwarzanych w systemie teleinformatycznym;
 - 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 teleinformatycznego, w którym są przetwarzane dane osobowe.

Rozdział 13

Realizacja obowiązku informacyjnego i praw osób, których dane dotyczą

§ 26.

1. Właściciel zbioru/ Dyrektor oddziału regionalnego odpowiada za realizację obowiązku informacyjnego zgodnie z art. 13 ust. 1 i 2 RODO, chyba że osoba, której dane dotyczą dysponuje już wszystkimi informacjami.
2. Obowiązek, o którym mowa w ust. 1, jest realizowany przez Właściciela zbioru/Dyrektora oddziału regionalnego poprzez udostępnienie w odpowiedni sposób klauzuli informacyjnej opracowanej na podstawie wzorów klauzul informacyjnych przygotowanych i opublikowanych w sieci wewnętrznej na stronie intranetowej Agencji przez Inspektora Ochrony Danych.
3. Właściciel zbioru/Dyrektor oddziału regionalnego danych odpowiada za realizację obowiązku informacyjnego w przypadku pozyskiwania danych osobowych w sposób inny niż bezpośrednio od osoby, której dane osobowe dotyczą, zgodnie z art. 14 ust. 1-3 RODO, mając również na względzie wyłączenia tego obowiązku przewidziane w art. 14 ust. 5 RODO.
4. 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, prawo do sprzeciwu

oraz prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, zgodnie z art. 15-22 RODO.

5. Każda osoba, której dane dotyczą ma prawo do cofnięcia wyrażonej przez siebie zgody w każdym dowolnym momencie i bez podawania przyczyny, zgodnie z art. 7 RODO. Jeżeli osoba, której dane osobowe dotyczą, skutecznie cofnęła zgodę, Administrator danych niezwłocznie zaprzestaje przetwarzania danych osobowych w celach, dla których zgodę pozyskiwał, a jeżeli nie ma innej podstawy prawnej do przetwarzania danych osobowych, usuwa te dane osobowe.
6. 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.
7. W razie skierowania wniosku do niewłaściwej jednostki lub komórki organizacyjnej Agencji, pracownik, który otrzymał wniosek, zobowiązany jest niezwłocznie, nie później niż w ciągu dwóch dni roboczych, w których wniosek wpłynął, przekazać go do właściwej jednostki lub komórki organizacyjnej.
8. W przypadku, gdy brak jest możliwości jednoznacznej weryfikacji tożsamości Wnioskodawcy, należy zażądać dodatkowych informacji w celu potwierdzenia jego tożsamości.
9. W przypadku, gdy brak jest możliwości jednoznacznego określenia faktycznej treści żądania Wnioskodawcy, należy zwrócić się do Wnioskodawcy o uzupełnienie wniosku o dodatkowe wyjaśnienia (sprecyzowanie żądania).
10. 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”, opracowywane i udostępniane w wewnętrznej sieci intranetowej Agencji przez Inspektora Ochrony Danych.
11. 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.
12. 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.
13. 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.
14. 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.
15. W razie potrzeby termin, o którym mowa w ust. 14, 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.

16. 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.
17. O odmowie podjęcia działań, z uwagi na okoliczności, o których mowa w ust. 16, Właściciel zbioru/Dyrektor oddziału regionalnego informuje osobę, której dane dotyczą w terminie miesiąca od otrzymania wniosku. Odpowiedź skierowana do osoby, której dane dotyczą, poza powodami niepodjęcia działań w związku ze złożonym wnioskiem, o których mowa w ust. 16, powinna zawierać informację o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej.
18. Każdy wniosek, o którym mowa w ust. 4 i 5 powyżej winien zostać odnotowany w rejestrze wniosków o realizację praw osób, których dane dotyczą. Wzór rejestru wniosków stanowi załącznik nr 5 do niniejszego regulaminu.

Rozdział 14

Udostępnianie danych osobowych

§ 27.

1. Dane osobowe udostępniane są na wniosek podmiotu zewnętrznego. Przekazywanie danych pomiędzy komórkami i jednostkami organizacyjnymi ARiMR nie stanowi udostępnienia danych osobowych.
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, spełniający wymagania określone w porozumieniach o współpracy zawartych pomiędzy Prezesem ARiMR a Głównym Lekarzem Weterynarii oraz Prezesem ARiMR a związkami hodowców koni, 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, o którym mowa w ust. 6, 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 wg wytycznych, o których mowa w ust. 14. Wniosek organu egzekucyjnego może zostać przekazany przez Właściciela zbioru do załatwienia Dyrektorowi oddziału regionalnego.
10. 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 powinien być parafowany przez osobę zatrudnioną na stanowisku radcy prawnego.
11. W przypadku, gdy załatwienie wniosku o udostępnienie danych osobowych w Centrali ARiMR wymaga przekazania danych przez kilku Właścicieli zbiorów, komórka właściwa ds. bezpieczeństwa w Centrali ARiMR koordynuje realizację takiego wniosku poprzez wskazanie komórki wiodącej, właściwej do zebrania informacji merytorycznej i stanowiska od Właścicieli zbiorów w zakresie powierzonych im danych, a następnie do udzielenia odpowiedzi wnioskodawcy.
12. Właściciel zbioru/Dyrektor oddziału regionalnego 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/Dyrektor oddziału regionalnego.
13. Dyrektor komórki właściwej ds. bezpieczeństwa prowadzi wykaz osób wyznaczonych, które podlegają okresowemu szkoleniu. Za przekazywanie informacji niezbędnych do

prowadzenia aktualnego wykazu odpowiadają Właściciele zbiorów/Dyrektorzy oddziałów regionalnych.

14. Dane osobowe udostępnia się na wniosek sporządzony w formie pisemnej lub elektronicznej, spełniający wymagania formalne oraz merytoryczne, 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.
15. Informacje zawierające dane osobowe są udostępniane uprawnionym podmiotom:
 - 1) w formie pisemnego wydruku, listem poleconym lub za potwierdzeniem osobistego odbioru;
 - 2) za pomocą usługi e-doręczenia, tj. rejestrowanego doręczenia elektronicznego, która umożliwia wysyłanie i odbieranie korespondencji elektronicznie, ze skutkiem równoważnym z listem poleconym za potwierdzeniem odbioru;
 - 3) za pomocą elektronicznej skrzynki podawczej e-PUAP – z użyciem podpisu kwalifikowanego lub potwierdzonego profilem zaufanym;
 - 4) w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych, np. poprzez plik zabezpieczony hasłem (z zachowaniem zabezpieczenia polegającego na przekazaniu hasła odrębnym kanałem komunikacji);
 - 5) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru;
 - 6) w inny sposób określony przepisami prawa lub umową.
16. Zawartość elektronicznych nośników informacji podlega kontroli i pisemnej akceptacji bezpośredniego przełożonego - osoby przygotowującej informację określoną w ust. 15.
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 teleinformatycznym. Ewidencję prowadzą:
 - 1) w Centrali Agencji – Właściciel zbioru;
 - 2) w oddziale regionalnym – Dyrektor;
 - 3) w biurze powiatowym – Kierownik.

Rozdział 15

Powierzenie przetwarzania danych osobowych innym podmiotom

§ 28.

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. Właściciel zbioru/Dyrektor oddziału regionalnego, korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia

odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów o ochronie danych osobowych (RODO) i chroniło prawa osób, których dane dotyczą.

4. W celu weryfikacji wypełniania przez potencjalny podmiot przetwarzający obowiązków, o których mowa w ust. 3, przed zawarciem umowy powierzenia przetwarzania danych, Właściciel zbioru/Dyrektor oddziału regionalnego zobowiązuje go do wypełnienia ankiety, której formularz stanowi załącznik nr 6 do niniejszego regulaminu. Jeżeli postępowanie jest prowadzone zgodnie z ustawą Prawo zamówień publicznych, ankietę należy dołączyć do SWZ.
5. Kandydat na podmiot przetwarzający jest oceniany na podstawie oświadczeń zawartych w ankiecie, w zakresie przestrzegania wymogów prawa, wiedzy fachowej w dziedzinie ochrony danych osobowych oraz wiarygodności, z uwzględnieniem kalkulatora dołączonego do arkusza oceny. Arkusz oceny podmiotu przetwarzającego jest opracowywany i udostępniany, a w razie konieczności aktualizowany przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.
6. Ostateczną decyzję o wyborze podmiotu przetwarzającego w imieniu Administratora danych podejmuje Właściciel zbioru/Dyrektor oddziału regionalnego. W razie potrzeby Inspektor Ochrony Danych przekazuje zalecenia, czy w jego ocenie dany kandydat na podmiot przetwarzający spełnia wymogi określone przepisami RODO.
7. 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.
8. Wzór umowy powierzenia przetwarzania danych osobowych jest opracowywany i udostępniany, a w razie konieczności aktualizowany przez Inspektora Ochrony Danych w sieci wewnętrznej na stronie intranetowej Agencji.

9. Ostateczny projekt umowy powierzenia przetwarzania danych osobowych, a także każdej innej umowy zawartej w Centrali Agencji, której realizacja wiąże 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.
10. 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) osoby zajmującej samodzielne stanowisko radcy prawnego w OR;
 - 4) Dyrektora OR.
11. Po zawarciu umowy powierzenia przetwarzania danych osobowych, komórka organizacyjna Centrali Agencji nadzorująca proces przygotowania umowy, niezwłocznie informuje wszystkich Właścicieli zbiorów, których dane są powierzane, o zawarciu przedmiotowej umowy oraz Dyrektora komórki właściwej ds. bezpieczeństwa.
12. 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.
13. Nadzór, o którym mowa w ust. 12, polega w szczególności na weryfikacji sposobu wykonywania Umowy Powierzenia przez Podmiot przetwarzający, w tym sprawdzaniu czy środki techniczne i organizacyjne zabezpieczające przetwarzanie powierzonych danych, zastosowane przez Podmiot przetwarzający, odpowiadają ryzyku naruszenia praw lub wolności osób, których dane dotyczą.
14. Właściciele zbiorów i Dyrektorzy oddziałów regionalnych prowadzą wykaz umów powierzenia przetwarzania danych według wzoru stanowiącego załącznik nr 7 do niniejszego regulaminu.

Rozdział 16

Postępowanie w przypadku kontroli PUODO

§ 29.

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, Właściciel rejestru czynności przetwarzania, 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. Administrator 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) Właściciel rejestru czynności przetwarzania;
 - 3) Administrator Systemu;
 - 4) Administrator Zabezpieczeń Fizycznych;
 - 5) Inspektor Ochrony Danych;
 - 6) Dyrektor komórki właściwej ds. bezpieczeństwa;
 - 7) kierownik komórki organizacyjnej, w której są przetwarzane dane osobowe;
 - 8) 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 17

Odpowiedzialność za naruszenie zasad ochrony danych osobowych

§ 30.

1. Naruszenie przepisów o ochronie danych osobowych może skutkować wyciągnięciem konsekwencji wobec osób zatrudnionych lub wykonujących zadania na rzecz ARiMR – zgodnie z treścią postanowień umownych oraz przepisów ogólnych, w szczególności Kodeksu cywilnego.
2. Naruszenie przepisów o ochronie danych osobowych może skutkować wyciągnięciem konsekwencji wobec osób zatrudnionych na podstawie umów cywilnoprawnych oraz osób związanych z Administratorem danych inną umową – zgodnie z treścią postanowień tych umów oraz przepisów ogólnych, w szczególności Kodeksu cywilnego.

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 A

Znak sprawy:

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, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35) zwanego dalej: „Rozporządzeniem”, upoważniam:

Panią/Pana*.....,

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

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

w zakresie niezbędnym do wykonywania powierzonych pracy****

Niniejsze upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w okresie wykonywania pracy w Agencji Restrukturyzacji i Modernizacji Rolnictwa.

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 2019 r., poz. 1781), ustawy z dnia 26.06.1974 r. *Kodeks Pracy* 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 składającej
oświadczenie)

Pouczenie:

* - wypełnić wstawiając: imię i nazwisko, indywidualny numer pracownika nadany w systemie kadrowo-płacowym ARiMR (KIP).

Dla innej osoby niż pracownik: imię i nazwisko, określenie statusu prawnego (np. wolontariusz, stażysta, praktykant, zleceniobiorca itp.).

** - niewłaściwe skreślić.

*** - 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.

Znak sprawy:

Wykaz osób upoważnionych do przetwarzania danych poza zbiorami w Centrali ARiMR/..... OR ARiMR*								
Lp.	Imię i Nazwisko	Jednostka org.	Komórka org.**	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

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, str. 1, Dz. Urz. UE. L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35),

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, pieczętka imienna i podpis Właściciela zbioru/Dyrektora OR)*

* Niepotrzebne skreślić

Znak sprawy:

	REJESTR WNIOSKÓW O REALIZACJĘ PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ							
L.p.	Komórka organizacyjna/imię i nazwisko pracownika rozpatrującego wniosek	Imię i nazwisko oraz adres Wnioskodawcy	Forma wniosku (w jaki sposób zgłoszono żądanie)	Przedmiot wniosku (ogólny opis czego dotyczy żądanie)	Sposób rozpatrzenia wniosku	Data wpływu wniosku do ARiMR	Termin rozpatrzenia wniosku	Dodatkowe uwagi
1.								
2.								
3.								
...								

Znak sprawy:

ANKIETA – WYMAGANIA DLA PODMIOTU ZEWNĘTRZNEGO w zakresie możliwości powierzenia przetwarzania danych osobowych

Poniższa ankieta ma na celu ustalenie czy Podmiot zewnętrzny, któremu ARiMR zamierza powierzyć przetwarzanie danych osobowych, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. W tym celu należy odpowiedzieć na poniższe pytania.

1. SYSTEMY OCHRONY DANYCH, KODEKSY POSTĘPOWANIA, CERTYFIKACJA

- 1) Czy Podmiot zewnętrzny ma wdrożony system zarządzania bezpieczeństwem informacji lub znak jakości i oznaczeń w zakresie ochrony danych osobowych, o których mowa w art. 42 RODO, i które obejmują całość operacji przetwarzania danych w ramach realizacji Umowy?

TAK/NIE

- 2) Czy Podmiot zewnętrzny wdrożył i stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO?

TAK/NIE

- 3) Czy system ochrony danych osobowych Podmiotu zewnętrznego był poddawany w ciągu ostatnich 3 lat sprawdzeniu przez audytorów zewnętrznych i uzyskał pozytywną opinię w tym zakresie (np.: posiada certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z normą ISO/IEC 27001 w pełnym zakresie)?

TAK/NIE

1.1. Wymagania do pkt 1

- a) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia **kopii certyfikatu**, o którym mowa w pytaniu pkt 3.
- b) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 1 lub 2 przy jednoczesnej negatywnej odpowiedzi na pytanie pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia obowiązujących w organizacji odpowiednio: **kodeksu postępowania** lub **zasad ochrony danych osobowych** (np. polityki bezpieczeństwa informacji).

W przypadku negatywnych odpowiedzi na pytania zawarte w pkt 1 – 3 należy odpowiedzieć na pytania zawarte w kolejnych punktach.

2. STRUKTURA OCHRONY DANYCH, DOŚWIADCZENIE

- 1) Czy Podmiot zewnętrzny posiada doświadczenie w świadczeniu usług polegających na zarządzaniu zbiorami danych osobowych w imieniu innego podmiotu (pełnił rolę podmiotu przetwarzającego)?

TAK*/NIE

* Jeśli TAK, to proszę wskazać dla ilu podmiotów była taka usługa świadczona i przez jaki okres (łącznie, np.: 5 podmiotów, 8 lat):.....

- 2) Czy w trakcie świadczenia usług, o których mowa w pytaniu zawartym w pkt 1 doszło do naruszenia ochrony danych osobowych w zakresie powierzonych danych z winy podmiotu przetwarzającego?

TAK/NIE/NIE DOTYCZY

- 3) Czy Podmiot zewnętrzny wyznaczył w strukturach wewnętrznych Inspektora Ochrony Danych lub osobę/komórkę odpowiedzialną za nadzór nad ochroną danych osobowych? (właściwe zaznaczyć)

TAK – Inspektor Ochrony Danych (IOD)	
TAK – osoba (inna niż IOD)/ komórka odpowiedzialna za ochronę danych osobowych	
NIE	

- 4) Czy Podmiot zewnętrzny opracował i wdrożył metodykę oraz procedury zarządzania ryzykiem związanym z bezpieczeństwem informacji w tym metodykę oraz procedury przeprowadzania oceny skutków dla ochrony danych?

TAK/NIE

- 5) Czy Podmiot zewnętrzny prowadzi rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO?

TAK/NIE

- 6) Czy Podmiot zewnętrzny prowadzi rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO?

TAK/NIE

- 7) Czy Podmiot zewnętrzny przeprowadza regularne (co najmniej raz w roku) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?

TAK/NIE

- 8) Czy Podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, określonych w art. 15 - 22 RODO?

TAK/NIE

3. ZASADY OCHRONY DANYCH

3.1. DOSTĘP DO DANYCH

- 1) Czy Podmiot zewnętrzny zapewnia, aby każdy nowozatrudniony pracownik przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami o ochronie danych osobowych, w tym wewnętrznymi?

TAK/NIE

- 2) Czy podmiot przetwarzający prowadzi cykliczne szkolenia doskonalące dla swojego personelu lub podejmuje inne działania mające na celu podnoszenie świadomości pracowników i uaktualnianie wiedzy z zakresu ochrony danych osobowych?

TAK/NIE

- 3) Czy osoby wykonujące operacje na danych osobowych otrzymały stosowne upoważnienia do przetwarzania danych, spełniające wymogi przepisu art. 29 RODO?

TAK/NIE

- 4) Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania ich w tajemnicy/poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy? Czy zostało to udokumentowane?

TAK (bez dokumentacji)	
TAK – udokumentowane	
NIE	

- 5) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury nadawania uprawnień do systemów teleinformatycznych przetwarzających dane osobowe, z zachowaniem zasad „wiedzy koniecznej”?

TAK/NIE

- 6) Czy Podmiot zewnętrzny prowadzi cykliczne przeglądy nadanych uprawnień?

TAK/NIE

- 7) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury bezzwłocznego odbierania uprawnień do systemów teleinformatycznych przetwarzających dane osobowe, w stosunku do osób, dla których ustała celowość dostępu?

TAK/NIE

3.2. FIZYCZNY DOSTĘP DO OBSZARÓW PRZETWARZANIA

- 1) Czy Podmiot zewnętrzny stosuje środki kontroli dostępu fizycznego do budynku/budynków ograniczające dostęp tylko dla autoryzowanego personelu?

TAK/NIE

- 2) Czy podmiot przetwarzający posiada odpowiednio wyposażone i zabezpieczone pomieszczenia umożliwiające bezpieczne przetwarzanie danych osobowych?

TAK/NIE

- 3) Czy Podmiot zewnętrzny zapewnia odpowiedni nadzór nad osobami niebędącymi jego pracownikami, a przebywającymi w jego siedzibie, także mających dostęp po godzinach pracy (personel sprzątający, personel ochrony fizycznej)?

TAK/NIE

- 4) Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?

TAK/NIE

3.3. OCHRONA DOMYŚLNA (PRIVACY BY DEFAULT)

- 1) Czy każdy pracownik otrzymuje unikalny identyfikator do systemów teleinformatycznych?

TAK/NIE

- 2) w systemach teleinformatycznych Podmiotu zewnętrznego zapewniono wymuszanie na użytkownikach stosowania haseł o odpowiedniej sile (kombinacja liter, cyfr i znaków specjalnych, min. 8 znakowe), także ich okresowej zmiany oraz zmian w razie zaistniałej potrzeby?

TAK/NIE

- 3) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego ekranu” polegającą na automatycznym wygaszaniu ekranu i blokowaniu systemu, po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła?

TAK/NIE

- 4) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego biurka” polegającą na obowiązku chowania dokumentów zawierających dane osobowe do zamykanych szaf na koniec dnia pracy?

TAK/NIE

- 5) Czy w systemach teleinformatycznych Podmiotu zewnętrznego wykorzystywane jest jedynie oprogramowanie autoryzowane przez Kierownictwo Podmiotu zewnętrznego?

TAK/NIE

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

TAK/NIE

- 7) Czy systemy teleinformatyczne Podmiotu zewnętrznego są objęte rzeczywistą ochroną przed szkodliwym oprogramowaniem (zainstalowane i regularnie uaktualniane oprogramowanie antymalwerowe na wszystkich urządzeniach wykorzystywanych do przetwarzania danych, w tym telefonach komórkowych)?

TAK/NIE

- 8) Czy Podmiot zewnętrzny posiada wdrożony proces zarządzania podatnościami technicznymi, mający na celu redukcję podatności, które mogą być wykorzystane przez szkodliwe oprogramowanie lub umożliwić atak hackerski?

TAK/NIE

- 9) Czy posiadane przez Podmiot zewnętrzny sieci komputerowe, zarówno przewodowe jak i bezprzewodowe, poprzez odpowiednią konfigurację urządzeń i systemów, umożliwiają blokowanie podejrzanego transmisji danych?

TAK/NIE

- 10) Czy urządzenia mobilne (laptopy, tablety, telefony komórkowe, itp.) wykorzystywane do przetwarzania danych osobowych, którymi Podmiot zewnętrzny dysponuje, są szyfrowane?

TAK/NIE

- 11) Czy jest stosowane szyfrowanie komunikacji pomiędzy systemami Podmiotu zewnętrznego?

TAK/NIE

- 12) Czy Podmiot zewnętrzny posiada wdrożone procedury bezpiecznego zbywania sprzętu, uwzględniające całkowite usuwanie danych z nośników informacji?

TAK/NIE

- 13) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania incydentami związanymi z bezpieczeństwem informacji?

TAK/NIE

- 14) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania ciągłością działania?

TAK/NIE

3.4. OCHRONA NA ETAPIE PROJEKTOWANIA (PRIVACY BY DESIGN)

- 1) Czy posiadane przez Podmiot zewnętrzny środowiska produkcyjne, testowe oraz deweloperskie są niezależne, odseparowane od siebie, przynajmniej na poziomie VLAN-ów?

TAK/NIE

- 2) Czy Podmiot zewnętrzny dokonuje dla każdego projektu (dotyczącego wytworzenia nowego oprogramowania, jak również zmiany istniejącego) szacowania ryzyka pod kątem bezpieczeństwa informacji?

TAK/NIE

- 3) Czy Podmiot zewnętrzny wdrożył i stosuje procedury odbioru systemów przed uruchomieniem na środowisku produkcyjnym, z uwzględnieniem aspektów bezpieczeństwa informacji?

TAK/NIE

3.5. Wymagania do pkt 2 i 3

Podmiot zewnętrzny zobowiązany jest do przedłożenia stosownych zasad, procedur, o których mowa w pkt 2 i 3.

4. WERYFIKACJA ZASAD OCHRONY DANYCH

- 1) W przypadku udzielenia odpowiedzi negatywnej na jakiekolwiek pytanie zawarte w pkt 2 oraz 3, czy Podmiot zewnętrzny wyraża gotowość do bezzwłocznego wdrożenia brakujących zasad?

TAK/NIE

- 2) Czy Podmiot zewnętrzny wyraża zgodę na ewentualną weryfikację w siedzibie Podmiotu zewnętrznego, opisanych powyżej zasad ochrony danych osobowych (sposób przeprowadzenia przez ARiMR audytu będzie uzgadniany indywidualnie)?

TAK/NIE

OŚWIADCZENIE

Działając w imieniu Podmiotu Przetwarzającego potwierdzam zgodność przedstawionych powyżej informacji pod rygorem odpowiedzialności prawnej, w tym odpowiedzialności wynikającej z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE. L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35).

.....

Data i podpis osoby upoważnionej

Znak sprawy:

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	Data zakończenia obowiązywania Umowy powierzenia przetwarzania	Strona Umowy powierzenia przetwarzania	Komórka organizacyjna nadzorująca wykonanie Umowy	Właściciel zbioru oraz zbiór danych podlegający powierzeniu	Uwagi
1	2	3	4	5	6	7	8

* Wypełnić właściwe, niepotrzebne skreślić.

** Dotyczy umowy, do której zawarto umowę powierzenia przetwarzania danych osobowych.