POLITYKA OCHRONY DANYCH OSOBOWYCH

w

Stowarzyszeniu Lokalna Grupa Działania „Gryflandia”

HISTORIA ZMIAN

DATA	WERSJA	WPROWADZIŁ	OPIS ZMIAN
[29.05.2018]	1	Mal	Pierwsza wersja dokumentu
[23.09.2019]	2	Mal	Rewizja dokumentu
[14.04.2020]	3	Mal	Rewizja dokumentu

Spis treści

I. Informacje ogólne

1. Głównym celem wprowadzenia Polityki Ochrony Danych Osobowych jest zapewnienie zgodności działania Stowarzyszenia Lokalna Grupa Działania „Gryflandia" jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Ochrony Danych Osobowych opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. Dokument Polityki Ochrony Danych Osobowych został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   - Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych [Dz.U. 2018 poz. 1000];
   - Rozporządzeniu 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 [RODO];
   - Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (U. 2004 nr 100 poz. 1024),

3. Obszarem przetwarzania danych osobowych przez Stowarzyszenie Lokalna Grupa Działania „Gryflandia" jest każdorazowy adres siedziby Stowarzyszenia.

4. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w instrukcji zarządzania systemem informatycznym.

5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

6. Zastosowane procedury mają służyć osiągnięciu powyższych celów:

   1) Poufność danych – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
   2) Integralność danych – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

3) Dostępność danych – zapewnienie osiągalności danych i możliwości ich wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
4) Rozliczalność danych – zapewnienie, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,
5) Autentyczność danych – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
6) Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
7) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych;
8) Minimalizacja danych – przetwarzanie wyłącznie danych osobowych odpowiednich i stosownych do osiągnięcia celu ich zebrania. Dane osobowe przetwarzane są tylko w takim zakresie, który jest niezbędny dla osiągnięcia celu ich zebrania.
9) Ograniczenie przechowywania – dane osobowe przechowywane są 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 mogą być przechowywane przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, przy czym wdrożone zostały odpowiednie środki techniczne i organizacyjne wymagane w celu ochrony praw i wolności osób, których dane dotyczą.

7. Administrator Danych Osobowych gromadzi przetwarza dane osobowe w następujących celach:

1) Wykonywanie obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników);
2) Rekrutacja w zakresie kandydatów na stanowisko;
3) Realizacja zadań statutowych w stosunku do członków stowarzyszenia oraz innych osób korzystających ze świadczeń oferowanych przez Stowarzyszenie w szczególności Beneficjentów środków unijnych;
4) Wykonanie obowiązków prawnych i umownych LGD „Gryflandia” w zakresie realizacji LSR – art. 6 ust. 1 lit. c) RODO;
5) Dochodzenie ewentualnych roszczeń – art. 6 ust. 1 lit. f) RODO;
6) Zabezpieczenie informacji na wypadek potrzeby wykazania faktów lub okoliczności – art. 6 ust. 1 lit. f) RODO;

II. Definicje

1. Przez użyte w Polityce Ochrony Danych Osobowych określenia należy rozumieć:

   1) Polityka Ochrony Danych Osobowych – rozumie się przez to Politykę Ochrony Danych Osobowych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia”;

   2) Administrator Danych Osobowych **–** Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest Stowarzyszenie Lokalna Grupa Działania „Gryflandia”, które zgodnie z § 33 Statutu Stowarzyszenia reprezentowane jest przez Przewodniczącego Zarządu działającego samodzielnie lub dwóch członków Zarządu działających łącznie;

   3) Biuro – Biuro Stowarzyszenia Lokalna Grupa Działania „Gryflandia”;

   4) Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

   5) Dane wrażliwe – dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

   6) Dane genetyczne – dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

   7) Dane biometryczne – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

8) Dane dotyczące stanu zdrowia – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;

9) Dane karne – dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;

10) Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

11) Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

12) Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

13) Podmiot przetwarzający lub Procesor – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

14) Odbiorca – osoba fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem z wyłączeniem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;

15) RCPD lub Rejestr – Rejestr Czynności Przetwarzania Danych Osobowych;

16) Naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

17) Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych;

18) Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych [Dz.U. 2018 poz. 1000];

19) Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) z późniejszymi zmianami;

20) RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE [rozporządzenie ogólne o ochronie danych];

21) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

22) Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;

23) Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;

24) Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

25) System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

26) Bezpieczeństwo systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;

27) Administrator Systemu Informatycznego – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).

28) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.

29) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

III. Dokumenty powiązane

Dokumentem powiązanym z Polityką Ochrony Danych Osobowych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" jest, zgodnie z wymogami § 3 ust. 1 Rozporządzenia, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia".

IV. Cel i zakres Polityki

1. Przepisy o ochronie danych osobowych nakładają na Administratora Danych obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, a także zmianą, utratą, uszkodzeniem lub zniszczeniem. Celem niniejszej Polityki Ochrony Danych Osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla realizacji zadań statutowych Stowarzyszenia Lokalna Grupa Działania „Gryflandia" oraz dla bieżącej działalności Stowarzyszenia.

2. W Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" przetwarzane są przede wszystkim dane osobowe członków Stowarzyszenia, pracowników biura Stowarzyszenia oraz osób współpracujących ze Stowarzyszeniem na podstawie umów cywilnoprawnych. Stowarzyszenie, w związku z realizacją zadań statutowych, przetwarza także dane osobowe beneficjentów i wnioskodawców, a także dane uczestników szkoleń organizowanych przez Stowarzyszenie. Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.

3. Politykę Ochrony Danych Osobowych stosuje się przede wszystkim do:

1) Wszystkich informacji dotyczących danych pracowników Stowarzyszenia Lokalna Grupa Działania „Gryflandia” oraz osób współpracujących ze Stowarzyszeniem na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.

2) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.

3) Wszystkich danych dotyczących członków Stowarzyszenia Lokalna Grupa Działania „Gryflandia” oraz innych osób, które wypełniły deklarację członkowską zgodnie z § 11 ust 1 Statutu Stowarzyszenia.

4) Wszystkich informacji dotyczących danych wnioskodawców i beneficjentów korzystających ze wsparcia w ramach funduszy unijnych.

5) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.

6) Rejestru osób dopuszczonych do przetwarzania danych osobowych.

7) Innych dokumentów zawierających dane osobowe.

4. Zakres ochrony danych osobowych określony w Polityce Ochrony Danych Osobowych ma zastosowanie do systemów informatycznych Stowarzyszenia Lokalna Grupa Działania „Gryflandia”, w których są przetwarzane dane osobowe, a w szczególności do:

   1) Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.

   2) Wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

   3) Wszystkich osób świadczących pracę bądź usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

5. Do stosowania zasad określonych w Polityce Ochrony Danych Osobowych zobowiązani są wszyscy Użytkownicy danych, w tym w szczególności pracownicy Biura Stowarzyszenia, zleceniobiorcy, stażyści oraz wszelkie inne osoby mające dostęp do informacji podlegających ochronie, w tym zwłaszcza członkowie organów Stowarzyszenia Lokalna Grupa Działania „Gryflandia”.

6. Dla realizowania obowiązku rozliczalności, Administrator prowadzi Rejestr Czynności Przetwarzania, za które jest odpowiedzialny. Rejestr Czynności Przetwarzania musi być udostępniony Organowi nadzorczemu na jego żądanie. Rejestr Czynności Przetwarzania nie powinien być udostępniany innym podmiotom trzecim bez uzasadnionej konieczności. O

udostępnieniu Rejestru Czynności Przetwarzania podmiotom trzecim decyduje Administrator. Wzór Rejestru Czynności Przetwarzania Danych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" stanowi załącznik nr 1 do Polityki Ochrony Danych Osobowych.

V. Obowiązki i odpowiedzialność

1. Do najważniejszych obowiązków Administratora Danych należy:

   1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;
   2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Ochrony Danych Osobowych;
   3) Dopełnianie obowiązku informacyjnego w stosunku do osób, których dane są przetwarzane;
   4) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
   5) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;
   6) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   7) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
   8) Nadzór nad bezpieczeństwem danych osobowych;
   9) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   10) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
   11) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
   10) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
   11) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;

12) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;

13) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

14) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;

15) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

16) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;

17) Zarządzanie licencjami oraz procedurami ich dotyczącymi;

18) Prowadzenie profilaktyki antywirusowej.

2. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;

2) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;

3) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

4) Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;

5) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

6) Informowania Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;

7) Zapoznanie się z Polityką Ochrony Danych Osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Zarządzanie ochroną danych osobowych

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 29 RODO lub umowy powierzenia. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych.

VII. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Ochrony Danych Osobowych i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązującymi u Administratora Danych. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego załącznik nr 3 do Polityki Ochrony Danych Osobowych.

VIII. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 29 RODO.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
3. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora Danych podpisane oświadczenie użytkownika.
4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego załącznik nr 4 i 5 do Polityki Ochrony Danych Osobowych. Upoważnienia, o których mowa powyżej przechowywane są w Biurze.
5. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Wzór oświadczenia o odwołaniu upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 6 do Polityki Ochrony Danych Osobowych. Niezależnie od odwołania upoważnienia do przetwarzania danych, upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych, ustania członkostwa w Stowarzyszeniu lub w organie Stowarzyszenia, jeżeli nadanie upoważnienia związane było ze sprawowaniem funkcji w organie Stowarzyszenia.

IX. Ewidencja osób upoważnionych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" jest prowadzona przez Administratora Danych zgodnie ze wzorem formularza stanowiącym załącznik nr 2 do Polityki Ochrony Danych Osobowych w Stowarzyszeniu.

X. Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi

określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.

2. Powierzając przetwarzanie danych osobowych, Administrator Danych powinien w sposób wyraźny zaznaczyć, że udostępnione dane mogą być wykorzystane wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.
4. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania niniejszej Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.
5. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Stowarzyszenia Lokalna Grupa Działania „Gryflandia" za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Administratora Danych Osobowych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

XI. Udostępnianie danych osobowych osobom trzecim

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą lub w inny sposób, jeżeli wynika to z realizacji przepisów prawa.
2. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Administrator Danych Osobowych prowadzi ewidencję udostępnienia danych osobowych osobom trzecim według wzoru stanowiącego załącznik nr 8 do Polityki Ochrony Danych Osobowych.

XII. Dokonanie obowiązku informacyjnego

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:
   a. tożsamości Administratora oraz danych kontaktowe oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;
   b. celach przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania;
   c. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – o prawnie uzasadnionych interesach realizowanych przez Administratora lub przez stronę trzecią;
   d. Odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   e. gdy ma to zastosowanie - zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony;
   f. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
   g. prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   h. jeżeli przetwarzanie odbywa się na podstawie Zgody - o prawie do cofnięcia Zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   i. prawie wniesienia skargi do Organu nadzorczego;
   j. czy podanie danych jest dobrowolne lub obowiązkowe;
   k. ewentualnym zautomatyzowanym podejmowaniu decyzji, w tym o Profilowaniu.

XIII. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie Stowarzyszenia Lokalna Grupa Działania „Gryflandia”, z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych. Szczegółowy wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych znajduje się w załączniku nr 7 do Polityki Ochrony Danych Osobowych.
2. Dane osobowe w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia” przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.

3. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:
    A. Środki organizacyjne:
        - wdrożenie Polityki Ochrony Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Stowarzyszeniu;
        - ustalona, indywidualna procedura udzielania upoważnień przez Administratora Danych poprzedzonego szkoleniem z zakresu przepisów i zasad ochrony danych osobowych;
        - prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych, a także podmiotów, którym dane osobowe zostają udostępnione;
        - procedura postępowania w sytuacji naruszenia ochrony danych osobowych;
        - konieczność składania deklaracji poufności przez Użytkowników danych;
        - procedury przechowywania zbiorów danych;
    B. Środki techniczne:
        - Zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym;
        - Stacje robocze wyposażone są w indywidualną ochronę antywirusową;
        - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
    C. Środki ochrony fizycznej:
        - Pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników Biura Stowarzyszenia;
        - Drzwi zwykłe (niewzmacniane, nie przeciwpożarowe) do pomieszczeń, w których przetwarzane są dane osobowe znajdują się wewnątrz budynku w strefie ograniczonego dostępu;
        - Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie;
        - Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie;
        - Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

XIV. Sprawdzenie stanu systemu ochrony danych osobowych

1. Administrator Danych Osobowych raz w roku sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W powyższym zakresie Administrator Danych Osobowych przygotowuje sprawozdanie zgodnie z wzorem stanowiącym załącznik nr 9.
2. Okresowy przegląd Polityki Ochrony Danych Osobowych powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Stowarzyszenia oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

XV. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   1) Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   3) Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);
   3) Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

2) Inicjuje ewentualne działania dyscyplinarne;

3) Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;

4) Dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;

2) Zabezpiecza ewentualne dowody;

3) Ustala osoby odpowiedzialne za naruszenie;

4) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);

5) Inicjuje działania dyscyplinarne;

6) Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;

7) Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących załącznik nr 10 do Polityki Ochrony Danych Osobowych.

XVI. Zgodność

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Stowarzyszenia Lokalna Grupa Działania „Gryflandia", które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

XVII. Postanowienia końcowe

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

WZÓR

Załącznik nr 1
Rejestr Czynności Przetwarzania

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LP.	**Nazwa czynności przetwarzania**	**Jednostka organizacyjna**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Źródło danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	**Nazwa podmiotu przetwarzającego i dane kontakowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	**DPIA (jeśli tak, lokalizacja raportu)**	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1																
2																
3																
4																
5																

Załącznik nr 2
Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Numer upoważnienia	Nazwa zbioru danych	Nazwisko i imię osoby upoważnionej	Data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia / cofnięcia upoważnienia	UWAGI (przyczyna cofnięcia uprawnień)

WZÓR

Załącznik nr 3
Oświadczenie użytkownika

.....
(Data, miejscowość)

.....
(Imię i nazwisko Użytkownika)

.....
(Adres zamieszkania)

Ja niżej podpisana/-y oświadczam, iż:

Zostałam/-em przeszkolona/-y w zakresie ochrony danych osobowych i znane mi są regulacje prawne w zakresie ochrony danych osobowych oraz regulacje wewnętrzne zawarte w Polityce Ochrony Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym w Stowarzyszeniu Lokalna Grupa Działania „Gryflandia" oraz zobowiązuję się do ich przestrzegania.

Jednocześnie zobowiązuję się:

1. zachować w tajemnicy powierzone mi do przetwarzania dane osobowe;

2. chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

.....
(podpis Administratora Danych lub osoby reprezentującej Administratora Danych)

.....
(podpis Użytkownika)

WZÓR

Załącznik nr 4
Upoważnienie do przetwarzania danych osobowych (członkowie organów Stowarzyszenia)

…….
(Data, miejscowość)

Na podstawie art. 29 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.U.UE.L.2016.119.1) – dalej RODO (GDPR), niniejszym upoważniam do przetwarzania danych osobowych:

_____ (imię, nazwisko)

W związku z wykonywaniem obowiązków wynikających z powołania do pełnienia funkcji członka Rady Decyzyjnej/Zarządu Stowarzyszenia Lokalna Grupa Działania „Gryflandia";

Upoważniam _____ (imię i nazwisko) do przetwarzania danych osobowych zawartych w następujących zbiorach:

_____
_____
_____

Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie (w tym miejscu należy wskazać kategorie danych oraz operacje na danych osobowych, jakich może dokonywać upoważniony do przetwarzania danych osobowych):

_____
_____

Okres ważności upoważnienia: od: _____do:_____

……

(podpis osoby reprezentującej Administratora Danych)

Oświadczam, że zobowiązuję się do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczeń.

……
(podpis Użytkownika)

WZÓR

Załącznik nr 5
Upoważnienie do przetwarzania danych osobowych (pracownicy/zleceniobiorcy)

.....
(Data, miejscowość)

Na podstawie art. 29 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.U.UE.L.2016.119.1) – dalej RODO (GDPR), niniejszym upoważniam do przetwarzania danych osobowych:

_____ (imię, nazwisko)

_____ *(stanowisko)*

w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku/obowiązków wynikających z zawartej umowy cywilnoprawnej.

Upoważniam _____ (imię i nazwisko) do przetwarzania danych osobowych zawartych w następujących zbiorach:

_____
_____

Upoważnienie obejmuje uprawnienie do przetwarzania danych w zakresie (w tym miejscu należy wskazać kategorie danych oraz operacje na danych osobowych, jakich może dokonywać upoważniony do przetwarzania danych osobowych):

_____
_____

Okres ważności upoważnienia: od: _____do:_____

.....

(podpis osoby reprezentującej Administratora Danych)

Oświadczam, że zobowiązuję się do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczeń.

..... *(podpis Użytkownika)*

WZÓR

Załącznik nr 6
Odwołanie upoważnienia do przetwarzania danych osobowych

Na podstawie art. 29 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.U.UE.L.2016.119.1) – dalej RODO (GDPR), niniejszym upoważniam do przetwarzania danych osobowych:

z dniem ……..odwołuję upoważnienie nr……..

Dla Pani/Pana ……
(imię i nazwisko Użytkownika)

…… ……
(podpis Użytkownika) *(podpis osoby reprezentującej Administratora Danych)*

Załącznik nr 7
Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Polityka obowiązuje w Stowarzyszeniu Lokalna Grupa Działania Gryflandia, w pomieszczeniach, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej. Stowarzyszenie Lokalna Grupa Działania Gryflandia ma siedzibę przy ul. Nowy Świat 6, 72-300 Gryfice.

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	Pokój nr ……
2.	Wykaz pomieszczeń, w których znajdują się stacje robocze stanowiące element systemu informatycznego (jednostki robocze)	Pokój nr ……
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe)	Pokój nr ……
4.	Wykaz programów, w których przetwarzane są dane osobowe	Microsoft Office, Microsoft Excel / Lefthand / Płatnik
5.	Informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń.	Szafy zamykane na klucz, pokoje zamykane na klucz, komputery z indywidualnymi hasłami –zmiana nie rzadziej niż raz na 60 dni.

WZÓR

Załącznik nr 8
Ewidencja udostępnienia danych osobowych

Lp.	Data wydania	Dane odbiorcy	Zakres udostępnionych danych	Podpis osoby udostępniającej dane osobowe

WZÓR

Załącznik nr 9
Protokół ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

.....

(Data, miejscowość)

1) Oznaczenie administratora danych i adres jego siedziby:

.....

(podać pełną nazwę oraz adres)

2) Imię i nazwisko osoby reprezentującej administratora danych:

.....

3) Wykaz czynności podjętych przez administratora danych osobowych w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

……

4) Datę rozpoczęcia i zakończenia sprawdzenia:

……

5) Określenie przedmiotu i zakresu sprawdzenia:

……

6) Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……

……

……

……

7) Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

……

……

……

8) Wyszczególnienie załączników stanowiących składową część protokołu:

……

……

……

……

(Data, miejsce i podpis ADO)

WZÓR

Załącznik nr 10
Raport z naruszenia bezpieczeństwa danych osobowych

.....
(Data, miejscowość)

1. Data: ..... r. Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
.....

3. Lokalizacja zdarzenia (np. nr pokoju, nazwa pomieszczenia):
.....
.....4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące: .
.....
.....
.....5. Przyczyny wystąpienia zdarzenia:
.....
.....

6. Podjęte działania:
.....
.....
7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(*podpis osoby reprezentującej Administratora Danych)*