INSTRUKCJA ZARZADZANIA SYSTEMEM INFORMATYCZNYM STOWARZYSZENIA LOKALNA GRUPA DZIAŁANIA „ZIELONE SĄSIEDZTWO”

Podstawa prawna

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z pózn. zm.) oraz 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. Nr 100, poz. 1024 z pózn. zm.)

§1
Przepisy ogólne

1. Instrukcja zarządzania systemem informatycznym Stowarzyszenia Lokalna Grupa Działania „Zielone Sąsiedztwo”, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa przetwarzania danych osobowych” obowiązującą w Stowarzyszeniu Lokalna Grupa Działania „Zielone Sąsiedztwo”.

§2
Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

- **Stowarzyszeniu** – należy przez to rozumieć Stowarzyszenie Lokalna Grupa Działania „Zielone Sąsiedztwo”,
- **Administratorze Danych** – należy przez to rozumieć Prezesa Stowarzyszenia,
- **Administratorze Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do wdrażania oraz nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
- **Administratorze Systemu Informatycznego** – należy przez to rozumieć pracownika lub pracowników informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych przetwarzanych w systemie informatycznym,
- **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- **sieci lokalnej** – należy przez to rozumieć lokalną sieć teleinformatyczną,
- **sieci Internet** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne (Dz. U. z 2004 r., Nr 171, poz. 1800, z pózn. zm.).

§3

Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz.926 z pózn. zm.),
- polityką bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Lokalna Grupa Działania „Zielone Sąsiedztwo”,
- niniejszym dokumentem,
oraz posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 4 do Polityki bezpieczeństwa przetwarzania danych osobowych Stowarzyszenia Lokalna Grupa Działania „Zielone Sąsiedztwo”.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 2.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do aplikacji.
9. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Prezesa Stowarzyszenia z podaniem daty oraz przyczyny odebrania uprawnień.
10. Prezesa Stowarzyszenia zobowiązany jest pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło.
12. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. Rejestr stanowi załącznik nr 3,

§4
Zasady posługiwania się hasłami

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny,
a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
7. Przy wyborze hasła obowiązują następujące zasady:
- minimalna długość hasła - 8 znaków,
- zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.)
- należy stosować: hasła zwierające kombinacje liter i cyfr, hasła zawierające znaki specjalne: (.,();'@, #, & itp.) o ile system informatyczny i oprogramowanie na to pozwala,
- zmiany hasła nie wolno zlecać innym osobom.

§5

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Rozpoczęciem pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
2. Przed opuszczeniu stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego.
3. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu
4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

§6

Procedury tworzenia kopii zapasowych

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
2. Kopie bezpieczeństwa wykonywane są co najmniej raz w roku.
3. Kopie bezpieczeństwa wykonywane są na płytach CD, DVD lub poprzez sieć lokalną na serwerach.
4. Zachowuje się minimum 20 kopii bezpieczeństwa z poprzednich dni.
5. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na płytach, DVD-R lub taśmach magnetycznych.
6. W przypadku wykonywania zabezpieczeń długoterminowych na taśmach magnetycznych lub płytach CD/DVD, nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności.

§7

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

1. Elektroniczne nośniki informacji:

- dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na dyskietkach, płytach CD/DVD czy dyskach twardych nie mogą opuścić obszaru przetwarzania danych osobowych.
- elektroniczne nośniki informacji są przechowywane w pokoju stanowiącym obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych, w zamkniętej szafie lub metalowych kasetach.
- urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny.
- elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika.
- urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
2. Kopie zapasowe.
- Kopie bezpieczeństwa są przechowywane w szafie w pomieszczeniu na I piętrze budynku Centrum Kultury i Inicjatyw Lokalnych w Podkowie Leśnej, wynajmowanym przez Stowarzyszenie Lokalna Grupa Działania „Zielone Sąsiedztwo”.
- Dostęp do danych opisanych w punkcie 1 ma Administrator Systemu Informatycznego oraz upoważnieni pracownicy.
3. Wydruki.
- W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
- Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
- Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§8
Sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem

- Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware.
- Każdy e-mail wpływający na konta pocztowe Stowarzyszenia musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.
- Bezwzględnie zabrania się pobierania z sieci Internet plików niewiadomego pochodzenia.
- Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
- Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze W przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
- W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

§9
Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
3. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

§10
Procedury wykonywania przeglądów i konserwacji systemu

1. Przeglądy i konserwacja urządzeń.
- Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
- Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.
2. Przegląd programów i narzędzi programowych.
- Konserwacja baz danych osobowych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
- Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób dostępu do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw.
- Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego”. Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 4.
- Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

§11
Połączenie do sieci Internet

Połączenie do sieci Internet jest realizowane poprzez sieć lokalną Stowarzyszenia LGD Zielone Sąsiedztwo z zastosowaniem zaawansowanych metod ochrony typu UTM.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym
Stowarzyszenia Lokalna Grupa
Działania „Zielone Sąsiedztwo”

OŚWIADCZENIE

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002r. Nr 101 poz. 926 z późn. zm.),

2. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024),

3. polityki bezpieczeństwa przetwarzania danych osobowych w Stowarzyszeniu Lokalna Grupa Działania „Zielone Sąsiedztwo”,

4. Instrukcji zarządzania systemem informatycznym w Stowarzyszeniu Lokalna Grupa Działania „Zielone Sąsiedztwo”.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:
1. zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Stowarzyszenia Lokalna Grupa Działania „Zielone Sąsiedztwo”, zabezpieczenia przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,

2. zachowaniem w tajemnicy, także po ustaniu stosunku pracy lub zaprzestaniu pełnienia funkcji w Stowarzyszeniu, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.

Podkowa Leśna, dn. . . . . .
(podpis pracownika)

Załącznik nr 2
do Instrukcji Zarządzania
Systemem
Informatycznym
Stowarzyszenia Lokalna Grupa
Działania „Zielone Sąsiedztwo”

WNIOSEKO NADANIE UPRAWNIEŃ
W SYSTEMIE INFORMATYCZNYM

Rodzaj zmiany w systemie informatycznym:

Nowy użytkownik □

Modyfikacja uprawnień □

Odebranie uprawnień □

Imię i nazwisko użytkownika	
Opis zakresu uprawnień użytkownika w systemie informatycznym	

Data wystawienia: . . . . . .

. . . . . .
(Podpis Prezesa Stowarzyszenia) (Akceptacja ABI)

Załącznik nr 3
do Instrukcji Zarządzania
Systemem
Informatycznym
Stowarzyszenia Lokalna Grupa
Działania „Zielone Sąsiedztwo”

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko i Imię (identyfikator)	System/aplikacja/zbiór danych osobowych	Data nadania upoważnienia	Data ustania uprawnień
1.				
2.				
3.				

Załącznik nr 4
do Instrukcji Zarządzania
Systemem
Informatycznym
Stowarzyszenia Lokalna Grupa
Działania „Zielone Sąsiedztwo”

DZIENNIK SYSTEMU INFORMATYCZNEGO
STOWARZYSZENIA LOKALNA GRUPA DZIAŁANIA
„ZIELONE SĄSIEDZTWO”

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu Informatycznego, a w szczególności:
- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

L.p.	**Data i godzina zdarzenia**	**Opis zdarzenia**	**Podjęte działania**	**Podpis**
1.				
2.				

Załącznik Nr 2 Do Polityki Bezpieczeństwa

w zakresie danych osobowych Stowarzyszenia LGD „Zielone Sąsiedztwo”

Wykaz osób upoważnionych do przetwarzania danych osobowych:

Członkowie Zarządu:

1. Łukasiewicz Anna
2. Latopolski Tomasz
3. Karolina Likhtarovich
4. Skajewska Adriana
5. Potkańska Barbara
6. Anna Kurman
7. Skalski Piotr
8. Zbigniew Musiałek
9. Grażyna Nowocień
10. Arnold Lis

Członkowie Rady:

1. Domaradzka Ewa
2. Witkowska Alina
3. Potkański Tomasz
4. Bułat Jakub
5. Cieślak Ewa
6. Agnieszka Wojcierowska
7. Joanna Pawlikowska
8. Ewa Chojecka
9. Milena Wach
10. Milena Wyszyńska
11. Marta Ostrowska
12. Łukasz Stępień
13. Paweł Chmieliński
14. Anna Kozłowska

Pracownicy biura LGD:

1. Dąbrówka Sylwia
2. Adriana Skajewska

Elżbieta Budkiewicz, właściciel Biura Rachunkowo PROFIT w Podkowie Leśnej.

Załącznik Nr 3 Do Polityki Bezpieczeństwa

w zakresie danych osobowych Stowarzyszenia LGD „Zielone Sąsiedztwo”

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nr ew.	Imię i nazwisko upoważnionego	funkcja	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Podpis osoby zatwierdzającej nadanie uprawnień

Załącznik Nr 4 Do Polityki Bezpieczeństwa

w zakresie danych osobowych Stowarzyszenia LGD „Zielone Sąsiedztwo”

Nr ewidencyjny: ....

(nadaje Pełnomocnik Danych Osobowych) (miejscowość) (data)

UPOWAŻNIENIE

do przetwarzania danych osobowych

I.Upoważniam Panią/Pana

.....

(imię i nazwisko)

zatrudnioną/zatrudnionego w

.....

.....

(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku:

.....

(zajmowane stanowisko)

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki,

ewidencje, rejestry, spisy itp.*) i elektronicznej, wg wykazu zbiorów podanych w pkt. II.

II.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:

1.....
.

2.....
.

3.....
.

.....

(podpis Administratora Danych Osobowych)

OŚWIADCZENIE PRACOWNIKA

III. Ja niżej podpisana (*ny*) oświadczam, iż:

1. Zostałam (*em*) przeszkolona (*ny*) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych t.j. Dz.U. z 2002 r. nr 101, poz. 926 z późn. zm. oraz „**Polityką Bezpieczeństwa Stowarzyszenia Lokalna Grupa Działania 'Zielone Sąsiedztwo'"** i wydanych na jej podstawie *„Instrukcji zarządzania systemem informatycznym".*

2. Zobowiązuję się:

· zachować w tajemnicy dane osobowe, z którymi zetknęłam się / zetknąłem się* w trakcie

wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy,

jak i po jego ustaniu;

· chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych,

zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

3. Znana jest mi odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54).

....

(podpis Pełnomocnika Lokalnego Administratora Danych) (data, podpis pracownika)

Uwaga:

- niniejsze upoważnienie zostało sporządzone w trzech jednobrzmiących egzemplarzach – każdy na prawach

oryginału, które otrzymują:

1. Osoba upoważniona;

2. Akta osobowe upoważnionego;

3. Administrator Danych Osobowych.

Zał. nr 4 do Regulaminu Biura Stowarzyszenia
Lokalna Grupa Działania „Zielone Sąsiedztwo”

……..……..
Imię i nazwisko

……
adres
…….
pesel

OŚWIADCZENIE DLA LGD

zgoda na przetwarzanie danych osobowych

☐ Wyrażam zgodę na przetwarzanie moich danych osobowych przez Stowarzyszenie LGD „Zielone Sąsiedztwo” dla potrzeb niezbędnych do realizacji celów LSR, monitoringu i ewaluacji, zgodnie z Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych (Dz. U. 2016 r. poz. 922 z późn. zm.).

☐ W zawiązku ze złożeniem przeze mnie w niniejszym naborze wniosku – operacji o dofinansowanie z Osi 4 LEADER w ramach Programu Rozwoju Obszarów Wiejskich (PROW) na lata 2014-2020, wyrażam zgodę na przetwarzanie moich danych osobowych.

☐ Przyjmuję do wiadomości, że moje dane osobowe przetwarzane będą przez Instytucję Zarządzającą PROW 2014-2020 oraz Instytucje wykonujące w jej imieniu zadania, a także przez Lokalną Grupę Działania „Zielone Sąsiedztwo” z siedzibą w Podkowie Leśnej zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami) w celach związanych z realizacją działań Programu Rozwoju Obszarów Wiejskich na lata 2014-2020.

☐ Przyjmuję do wiadomości, iż:

1. Przysługuje mi prawo wglądu do moich danych osobowych oraz do ich poprawiania.
2. Dane podmiotu ubiegającego się o przyznanie pomocy mogą być przetwarzane przez organy audytowe i dochodzeniowe Unii Europejskiej i państw członkowskich dla zabezpieczenia interesów finansowych Unii.
3. Dane podmiotu ubiegającego się o przyznanie pomocy oraz kwota pomocy (jeżeli dotyczy) będą publikowane na stronie internetowej www.zielonesasiedztwo.pl
4. Administratorem danych jest LGD Zielone Sąsiedztwo z siedzibą w Podkowie Leśnej ul. Lilpopa 18, Biuro; Podkowa Leśna ul. Świerkowa 1
5. Podanie danych osobowych jest dobrowolne, niemniej niepodanie danych wskazanych we wniosku uniemożliwia dalsze procedowanie.

Oświadczam, iż preferowaną formą szybkiej komunikacji w związku z aplikowaniem o środki jest:

- e-mail: ……...

Lub - tel: …….

---------- ----------