Polityka Bezpieczeństwa
w zakresie danych osobowych
Stowarzyszenia Lokalna Grupa Działania „Zielone Sąsiedztwo”

Polityka bezpieczeństwa określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Podstawa prawna

- Konstytucja Rzeczypospolitej Polskiej art. 47, 51;
- Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz. U. Nr 101 poz. 926 z 2002 r.);
- 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 2004).

Definicje

- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
- **Zbiór danych osobowych -** każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie; zwłaszcza takie, które wykonuje się w systemach informatycznych;
- **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje. Systemem informatycznym jest również system, w którym nie ma żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;
- **Bezpieczeństwo systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;
- **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem

danych jest Dyrektor jednostki, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;

- **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika 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;
- **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych przetwarzanych w systemie informatycznym;
- **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osoba uprawniona przez niego do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
- **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;
- **Sieć Lokalna (LAN** Local Area Network**)** – c;
- **Sieć rozległa (WAN)** – Rozległa sieć teleinformatyczna;
- **Identyfikator użytkownika (LOGIN) –** ciąg znaków literowych i cyfrowych, lub inny, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło (Password)–** ciąg znaków literowych, cyfrowych lub inny, znany jedynie osobie upoważnionej do pracy w systemie informatycznym;
- **Zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby, upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Cele

Celem wdrożenia polityki bezpieczeństwa jest ochrona systemu informatycznego jako całości, jego poszczególnych elementów, przetwarzanych przez system zbiorów danych, obszaru, w którym przetwarzane są dane osobowe, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.

Rozdział 1

Wykazy

1.1 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Dane osobowe przetwarzane są w siedzibie Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” w Podkowie Leśnej, przy ul. Świerkowej 1.

1.1.1 Pomieszczenia zabezpieczone są przed dostępem osób trzecich.

1.1.2 Dostawcy usług serwerowych zabezpieczają swoje pomieszczenia przed dostępem osób trzecich według wewnętrznych procedur.

1.1.3 Nośniki informacji są przechowywane w siedzibie Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” w Podkowie Leśnej, przy ul. Świerkowej 1.

1.2 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Dane osobowe przechowywane są i przetwarzane w formie dokumentów fizycznych, przy użyciu oprogramowania komputerowego oraz systemów wykorzystujących oprogramowanie internetowe.

1.2.1 Istnieją następujące fizyczne zbiory danych osobowych:

a) zbiór deklaracji członkowskich Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” o wzorze ustalonym przez Zarząd;

b) zbiór dokumentów związanych z naborami na środki w ramach PROW 2014-2020;

1.2.2 Dane osobowe przechowywane i przetwarzane są także przy wykorzystaniu platformy systemowej Windows (w wersji 10).

1.2.3 Dane osobowe przechowywane i przetwarzane są z wykorzystaniem oprogramowania Office w wersji 2007.

1.2.4 W każdym wypadku korzystania z systemów i oprogramowania wymienionych w punkcie 1.2.2 i 1.2.3 dostęp do danych chroniony jest według procedur opisanych w rozdziale 4 niniejszego dokumentu.

1.2.7 Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” korzysta z internetowych systemów przetwarzania danych.

1.2.8 Dane w systemie internetowym umieszczone są na wydzielonym serwerze i powierzone firmie Progreso z siedzibą w 44-330 Jastrzębie-Zdrój ul. 1 Maja 7, gdzie wszystkie usługi i procesy należą tylko do OMIKRON. Serwer mieści się w budynku DATA CENTER operatora Atman w Katowicach.

1.2.9 Programem służącym do przetwarzania zbioru danych w systemie internetowym: OMIKRON Nabory

1.2.10 Dane umieszczone są w postaci pików w folderze o nazwie podkowa oraz w wydzielonej bazie danych MySQL o tej samej nazwie. Dane nie są współdzielone z danymi innych podmiotów i są umieszczone w tabelach.

1.2.11 Aplikacją służącą do przetwarzania zbioru danych jest OMIKRON Nabory

Rozdział 2

Osoby przetwarzające dane osobowe

2.1 Osoby upoważnione do przetwarzania danych osobowych

2.1.1 Do przetwarzania danych osobowych członków Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo" uprawniony jest Prezes i pracownicy Biura.

2.1.2 Do przetwarzania danych osobowych osób składających wniosek o pomoc oraz beneficjentów PROW uprawniony jest Zarząd, Rada Stowarzyszenia, Komisja Rewizyjna oraz pracownicy Biura Stowarzyszenia w zakresie niezbędnym dla realizacji naboru.

2.1.3 Uprawnienia, których zakres wymieniają punkty od 2.1.1 i 2.1.2, nadawane są poprzez automatyczne naniesienie danych osoby upoważnionej do przetwarzania danych osobowych do Ewidencji oraz przez wystawienie Upoważnienia do przetwarzania danych osobowych, którego kopię osoba ta winna podpisać i złożyć u Prezesa Stowarzyszenia.

2.1.4 Za datę nadania uprawnień rozumie się datę wpisania osoby do Ewidencji.

2.1.5 Za datę wygaśnięcia uprawnień przyjmuje się datę końca pełnienia funkcji przez osobę powołującą.

2.2 Ewidencja osób przetwarzających dane osobowe

2.2.1 Zgodnie z art. 39 ustawy administrator danych prowadzi Ewidencję osób upoważnionych do ich przetwarzania.

2.2.2 Ewidencja zawiera:

a) imię i nazwisko osoby upoważnionej,

b) funkcję osoby upoważnionej ,

c) datę nadania i datę ustania upoważnienia,

d) zakres upoważnienia do przetwarzania danych osobowych,

e) podpis osoby stwierdzającej nadanie uprawnień.

2.2.3 Ewidencja prowadzona jest przez Administratora danych osobowych.

2.4 Obowiązki osoby przetwarzającej dane.

2.4.1 Każda osoba uprawniona do przetwarzania danych osobowych w Stowarzyszeniu Lokalna Działania „Zielone Sąsiedztwo" w jakimkolwiek zakresie zobowiązana jest zapoznać się z Polityką bezpieczeństwa Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo" oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i postępować zgodnie z nimi.

2.4.2 W szczególności na każdą osobę wchodzącą w posiadanie danych osobowych nałożony jest obowiązek zachowania tych danych w tajemnicy zarówno w momencie posiadania uprawnień do

administrowania danymi, jak i po ustaniu tego uprawnienia, pod groźbą odpowiedzialności karnej.

2.4.3 Upoważnienie, o którym mowa w punkcie 2.1.3, przechowywane jest w Archiwum Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo”.

Rozdział 3

Przepływ danych

3.1 Sposób przepływu danych pomiędzy poszczególnymi systemami

3.1.1 Administrator dopuszcza przepływ danych między poszczególnymi systemami.

3.1.2 W szczególności dopuszczalne jest gromadzenie danych pochodzących z dokumentów fizycznych pod postacią dokumentów elektronicznych, przy czym forma dokumentu elektronicznego odpowiada dokumentowi fizycznemu.

3.1.3 Dopuszczalne jest tworzenie elektronicznych raportów, zestawień i baz służących realizacji zadań statutowych przez organy Stowarzyszenia. W szczególności możliwe jest tworzenie elektronicznego zestawienia danych pochodzących z dokumentów, o których mowa w punkcie 2.1.1 i 2.1.2 niniejszego dokumentu.

Rozdział 4

Środki techniczne zapewniające poufność danych

4.1 Zagadnienia wstępne

4.1.1 Celem zabezpieczenia zbiorów danych osobowych przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne.

4.1.2 Rozdział ten określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

4.2 Fizyczne zbiory danych

4.2.1 Fizyczny zbiór danych osobowych przechowywany jest w formie uporządkowanej. Dla deklaracji członkowskich stosuje się numer deklaracji.

4.2.2 Fizyczny zbiór danych osobowych przechowywany jest w sposób uniemożliwiający dostęp do niego osobom trzecim, to znaczy jest on przechowywany w zamkniętym pomieszczeniu, wymienionym w punkcie 1.1.

4.2.3 Wszystkie dokumenty fizyczne przechowywane są w sposób uniemożliwiający dostęp do nich osobom trzecim, bez wykorzystania nadmiernych sił i środków, mimo przebywania w pomieszczeniach, w których dane te są przechowywane. W szczególności oznacza to przechowywanie dokumentów w wolno stojącym lub zabudowanym meblu zamykanym na zamek, który otworzyć mogą wyłącznie uprawnione osoby.

4.3 Elektroniczne zbiory danych

4.3.1 Dokumenty przetwarzane są na urządzeniach znajdujących się w pomieszczeniach, o których mówi punkt 1.1.

4.3.2 Urządzenia powyższe zabezpieczone są przed kradzieżą.

4.3.3 Bezpośredni dostęp do danych jest zabezpieczony.

4.3.4 Zabezpieczenie, o którym mowa w punkcie 4.3.3 realizowane jest poprzez:

a) utworzenie osobnych kont dla użytkowników,

b) zabezpieczenia hasłem dostępu do plików.

4.3.5 Zabezpieczenie, o którym mowa w punkcie 4.3.4.a polega na utworzeniu nazwy użytkownika i hasła. Są one indywidualne dla każdej osoby uprawnionej do przetwarzania danych.

4.3.6 Przez hasło rozumie się minimum 8-znakową kombinację cyfr i liter, zgodną z postanowieniami ustawy i aktów wykonawczych. Jego zmiana następuje nie rzadziej niż co 30 dni. Dopuszcza się również możliwość uwierzytelniania za pomocą technologii biometrycznej.

4.3.7 W celu zabezpieczenia systemu i ochrony danych osobowych wprowadza się zabezpieczenie firewall, system izolacji selekcji połączeń z siecią zewnętrzną. Instalacja firewall jest obligatoryjna dla wszystkich urządzeń, na których przetwarzane są dane osobowe, a które połączone są z siecią zewnętrzną.

4.3.8 W celu zabezpieczenia systemu i ochrony danych osobowych wprowadza się zabezpieczenie antywirusowe. Korzystanie z takiego oprogramowania jest obowiązkowe.

4.3.9 Na osobie uprawnionej do przetwarzania danych osobowych spoczywa obowiązek dbania o aktualizacje oprogramowania wymienionego w punktach 4.3.7 i 4.3.8, a także samego systemu i oprogramowania, wymienionych w punktach 1.2.2 i 1.2.3.

4.3.10 Wszelkie nośniki danych znajdują się w pomieszczeniu wskazanym w punkcie 1.1 i są zabezpieczone przed ich wyniesieniem bądź zniszczeniem przez nieuprawnione osoby.

4.3.11 Dostęp do danych zgromadzonych na nośnikach, w szczególności nośnikach służących zapisywaniu kopii zapasowych, tj. płyt CD, DVD, dyskietek, urządzeń typu pendrive, dysków wymiennych jest uniemożliwiony osobom nieuprawnionym.

4.3.12 Jeśli istnieje konieczność serwisowania urządzeń, w obrębie których przechowywane są dane osobowe lub ich zbiory, zlecający usługę serwisowania zobowiązany jest do podpisania z serwisem umowy o zachowaniu tajemnicy danych osobowych.

4.5 Kopie zapasowe

4.5.1 Za sporządzenie kopii zapasowej danych odpowiada osoba bezpośrednio administrująca tymi danymi.

4.5.2 Osoba przetwarzająca dane osobowe w zbiorze tworzy kopie zapasowe tego zbioru w miarę potrzeb, nie rzadziej jednak niż raz w roku.

4.5.3 Kopia zapasowa danych przechowywana jest na nośniku zewnętrznym.

4.6 Przekazywanie danych

4.6.1 Dane mogą być przenoszone i przekazywane pomiędzy osobami posiadającymi uprawnienia do ich przetwarzania.

4.6.2 W chwili utraty uprawnień do przetwarzania danych osobowych, osoba tracąca uprawnienia zobowiązana jest niezwłocznie przekazać wszelkie zbiory danych będące w jej posiadaniu i ich kopie

swojemu następcy na funkcji zajmowanej w Stowarzyszeniu Lokalna Działania „Zielone Sąsiedztwo”.
4.6.3 Jeśli brak jest następcy, osoba, o której mowa w punkcie 4.6.2 przekazuje zbiory danych i ich kopie Prezesowi Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo”.

4.7 Przenoszenie danych
4.7.1 Możliwe jest przenoszenie danych osobowych i ich zbiorów.
4.7.2 Dane przenoszone winny być zabezpieczone przed dostępem osób trzecich, w szczególności:
a) fizyczne dokumenty winny być przenoszone w zabezpieczonych kopertach opisanych danymi kontaktowymi osoby przenoszącej dane,
b) nośniki dokumentów elektronicznych winny być przenoszone w sposób gwarantujący najwyższe bezpieczeństwo,
c) dane lub ich zbiory w formie fizycznej lub na nośnikach, w szczególności płytach CD, DVD, pendrive mogą być przesyłane za pośrednictwem poczty wyłącznie po zabezpieczeniu samego nośnika oraz po nadaniu przesyłki za potwierdzeniem odbioru.

4.8 Niszczenie danych
4.8.1 Dane osobowe i ich zbiory są przechowywane w Stowarzyszeniu Lokalna Działania „Zielone Sąsiedztwo” tak długo, jak ich przetwarzanie służy realizacji celów statutowych Stowarzyszenia.
4.8.2 Dane niszczone są wyłącznie, gdy są bezużyteczne i nie ma obowiązku ich przechowywania.
4.8.3 Osobą odpowiedzialną za zniszczenie danych jest Administrator Danych Osobowych.
4.8.4 Zniszczenie danych fizycznych polega na zniszczeniu dokumentów uniemożliwiającym ich ponowne odczytanie, w szczególności z wykorzystaniem niszczarki.
4.8.5 Zniszczenie danych elektronicznych polega na trwałym usunięciu tych danych, a jeśli to możliwe także sformatowaniu nośnika.
4.8.6 Zniszczenie danych odnotowuje się poprzez sporządzenie protokołu zniszczenia, który należy przechowywać we właściwym archiwum Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo”.
4.8.7 Wzór protokołu zniszczenia ustala Zarząd w drodze uchwały. Protokół ten zawiera w szczególności datę zniszczenia, informacje o danych lub ich zbiorze, przyczynę zniszczenia danych oraz podpisy osób uprawnionych do zniszczenia danych.

Rozdział 5
Postanowienia końcowe
5.1 We wszystkich kwestiach, których nie reguluje Polityka bezpieczeństwa Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” oraz instrukcja zarządzania systemem informatycznym zastosowanie mają przepisy ustawy i przepisy rozporządzenia.
5.2 Wszelkie zmiany dotyczące Polityki bezpieczeństwa Stowarzyszenia Lokalna Działania „Zielone Sąsiedztwo” podejmuje w drodze uchwały Zarząd Stowarzyszenia.
5.3 Dokument wchodzi w życie z dniem uchwalenia.

Załączniki do Polityki bezpieczeństwa Stowarzyszenia Lokalna Grupa Działania „Zielone Sąsiedztwo”:

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Stowarzyszeniu Lokalna Działania „Zielone Sąsiedztwo”,
2. Wykaz osób upoważnionych do przetwarzania danych osobowych,
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych,
4. Upoważnienie do przetwarzania danych osobowych w Stowarzyszeniu Lokalna Działania „Zielone Sąsiedztwo