POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

STOWARZYSZENIE RODZICÓW DZIECI
Z WRODZONĄ PRZEPUKLINĄ PRZEPONOWĄ
I INNYMI WADAMI WRODZONYMI
ORAZ ICH RODZIN
„ZUZIK”

Niniejsza polityka bezpieczeństwa stanowi zbiór wytycznych i instrukcji znajdujących zastosowanie w ochronie danych osobowych w Stowarzyszeniu Rodziców Dzieci z Wrodzoną Przepukliną Przeponową i Innymi Wadami Wrodzonymi oraz Ich Rodzin ”ZUZIK” w Kołobrzegu przy ulicy Zagłoby 24, 78-100. Dokument ten został sporządzony na podstawie przepisów ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. Nr 133, poz. 883 ze zm.) oraz rozporządzenia 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 ze. zm.).

I. Definicje Polityki Bezpieczeństwa

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1. **zbiorze danych** - 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;
2. **przetwarzaniu 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;
3. **systemie informatycznym** - rozumie się przez to, zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
4. **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to, wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
5. **usuwaniu danych** - rozumie się przez to, zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
6. **administratorze danych** - Stowarzyszenie Rodziców Dzieci z Wrodzoną Przepukliną Przeponową i Innymi Wadami Wrodzonymi oraz Ich Rodzin „ZUZIK", podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, zwany dalej „ZUZIK";
7. **administrator systemu informatycznego –** rozumie się przez to osobę albo podmiot odpowiedzialne za działanie oraz zabezpieczenie systemu informatycznego odpowiedzialną za bezpieczeństwo danych osobowych;
8. **zgodzie osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
9. **odbiorcy danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   - **9.1.** osoby, której dane dotyczą;
   - **9.2.** osoby upoważnionej do przetwarzania danych;
   - **9.3.** przedstawiciela, o którym mowa w art. 31a art. 31a ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych;
   - **9.4.** podmiotu, o którym mowa w art. 31 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych;
   - **9.5.** organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
10. **ustawie** - rozumie się przez to, ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
11. **identyfikatorze użytkownika** - rozumie się przez to, ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
12. **haśle** - rozumie się przez to, ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
13. **sieci telekomunikacyjnej** - rozumie się przez to, sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, ze zm.);
14. **sieci publicznej** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;

15. **teletransmisji** - rozumie się przez to, przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
16. **rozliczalności** - rozumie się przez to, właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
17. **integralności danych** - rozumie się przez to, właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
18. **raporcie** - rozumie się przez to, przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
19. **poufności danych** - rozumie się przez to, właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
20. **uwierzytelnianiu** - rozumie się przez to, działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
21. **osobie upoważnionej**- rozumie się przez to, osobę posiadającą formalne upoważnienie wydane przez „ZUZIK" (lub przez osobę wyznaczoną), uprawnioną do przetwarzania danych osobowych;

II. Cel i zasady Polityki Bezpieczeństwa

Polityka Bezpieczeństwa została ustanowiona w celu zapewnienia:

1. integralności danych osobowych,
2. rozliczalności danych osobowych,
3. pełnej ochrony danych osobowych przed pozyskaniem ich przez nieuprawniony podmiot,
4. zgodnego z prawem przetwarzania danych osobowych,
5. ochrony praw osób, których dotyczą przetwarzane dane osobowe.

III. Podmioty odpowiedzialne za realizację Polityki Bezpieczeństwa

§ 1

Naczelnymi podmiotami odpowiedzialnymi za realizację Polityki Bezpieczeństwa są Administrator Danych i Administrator Systemu Informatycznego.

1. Administrator Systemu Informatycznego jest wybierany zgodnie z postanowieniami niniejszej Polityki Bezpieczeństwa.

§ 2

Do obowiązków „ZUZIK" należy:

1. wdrażanie postanowień Polityki Bezpieczeństwa,
2. nadzorowanie administratora systemu oraz innych osób przetwarzających dane w zakresie realizacji Polityki Bezpieczeństwa,
3. nadzorowanie zabezpieczeń danych osobowych,
4. czuwanie nad prawidłowością przetwarzania danych osobowych,
5. wydawanie upoważnień osobom do przetwarzania danych osobowych,
6. prowadzenie ewidencji pomieszczeń służących do przetwarzania danych osobowych,

7. aktualizacja Polityki Bezpieczeństwa,
8. dokonywanie zgłoszeń rejestracyjnych oraz aktualizacyjnych danych osobowych,
9. podejmowanie interwencji w przypadku stwierdzenia naruszenia Polityki Bezpieczeństwa lub zagrożenia dla przetwarzanych danych osobowych.

§ 3

Administrator systemu informatycznego powoływany jest w formie uchwały Zarządu.

1. Powołanie na funkcję administratora systemu informatycznego jest równoznaczne z udzieleniem upoważnienia do przetwarzania danych osobowych.
2. Administrator Systemu Informatycznego odwoływany jest w formie uchwały Zarządu z pełnionej przez niego funkcji.
3. W przypadku odwołania administratora systemu informatycznego, nowy administrator systemu informatycznego powinien być powołany w terminie 7 dni.

§ 4

Do obowiązków Administratora Systemu Informatycznego należy:

1. zarządzanie systemem informatycznym,
2. wdrażanie rozwiązań technicznych w systemie informatycznym służących ochronie danych osobowych,
3. bieżąca konserwacja i nadzór nad prawidłowym działaniem systemu informatycznego,
4. na polecenie „ZUZIK", przydzielanie uprawnień do przetwarzania danych w systemie informatycznym,
5. na polecenie „ZUZIK", odbieranie uprawnień do przetwarzania danych w systemie informatycznym,
6. rejestrowanie naruszenia przepisów prawa lub Polityki Bezpieczeństwa w systemie informatycznym i informowanie o nich „ZUZIK",
7. przygotowanie kopii danych osobowych oraz ich zabezpieczenie,
8. zabezpieczenie nośników z danymi osobowymi,
9. nadzorowanie likwidacji nośników danych osobowych,
10. prowadzenie ewidencji upoważnionych osób,
11. składanie corocznych raportów Zarządowi Stowarzyszenia w zakresie realizacji Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

§ 5

Zarząd powierza funkcję Administratora Systemu Informatycznego osobie dysponującej wiedzą i doświadczeniem w zakresie administrowania systemem informatycznym.

1. Zarząd może powierzyć administrowanie systemem informatycznym innej osobie na podstawie zawartej z nią umowy cywilnoprawnej.

IV. Zabezpieczenia danych osobowych

§ 1

1. Dane osobowe zabezpiecza się przy użyciu środków zapewniających integralność i rozliczalność danych oraz chroniących dane przed nieuprawnionym pozyskaniem i przetwarzaniem.
2. W celu zapewnienie bezpieczeństwa danych osobowych Zarząd Stowarzyszenia określa poziom bezpieczeństwa danych osobowych, który zobowiązani są stosować „ZUZIK" oraz Administrator Systemu informatycznego.

§ 2

1. Podstawowy poziom bezpieczeństwa stosuje się, jeżeli żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną i w systemie informatycznym nie są przetwarzane dane osobowe ujawniające:
   1.1. pochodzenie rasowe lub etniczne,
   1.2. poglądy polityczne,
   1.3. przekonania religijne lub filozoficzne,
   1.4. przynależność wyznaniową, partyjną lub związkową,
   1.5. stan zdrowia,
   1.6. informacje o kodzie genetycznym, nałogach lub życiu seksualnym,
   1.7. informacje dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych,
   1.8. orzeczenia wydane w postępowaniu sądowym lub administracyjnym.
2. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
3. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   3.1. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   3.2. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
4. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
   4.1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   4.2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 90 dni. Hasło składa się co najmniej z 6 znaków.
7. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
8. Kopie zapasowe:
   8.1. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   8.2. usuwa się niezwłocznie po ustaniu ich użyteczności.

9. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przeznaczonym do przetwarzania danych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

10. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
- **10.1.** likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- **10.2.** przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- **10.3.** naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez „ZUZIK"

11. Administrator Systemu Informatycznego monitoruje wdrożone zabezpieczenia systemu informatycznego.

§ 3

1. Podwyższony poziom bezpieczeństwa stosuje się, jeżeli żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną i w systemie informatycznym są przetwarzane dane osobowe ujawniające:

1.1. pochodzenie rasowe lub etniczne,

1.2. poglądy polityczne,

1.3. przekonania religijne lub filozoficzne,

1.4. przynależność wyznaniową, partyjną lub związkową,

1.5. stan zdrowia,

1.6. informacje o kodzie genetycznym, nałogach lub życiu seksualnym,

1.7. informacje dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych,

1.8. orzeczenia wydane w postępowaniu sądowym lub administracyjnym.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Urządzenia i nośniki zawierające dane osobowe, o których mowa w rozdziale IV § 3 ust. 1 Polityki Bezpieczeństwa, przekazywane poza obszar przeznaczony do przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

4. Instrukcja zarządzania systemem informatycznym rozszerza się o sposób stosowania środków wskazanych w ustępie poprzedzającym.

5. Administrator Systemu Informatycznego stosuje na poziomie podwyższonym środki bezpieczeństwa określone w rozdziale IV § 2 Polityki Bezpieczeństwa, o ile zasady zawarte w niniejszym paragrafie nie stanowią inaczej.

§ 4

Wysoki poziom bezpieczeństwa stosuje się, jeżeli chociaż jedno urządzenie należące do systemu informatycznego jest podłączone do sieci publicznej.

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
   2.1. kontrolę przepływu informacji pomiędzy systemem informatycznym „ZUZIK" a siecią publiczną;
   2.2. kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego „ZUZIK"
3. Administrator Systemu Informatycznego stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
4. Administrator Systemu Informatycznego stosuje na poziomie wysokim środki bezpieczeństwa, określone w rozdziale IV § 2 i § 3 Polityki Bezpieczeństwa, o ile zasady zawarte w niniejszym paragrafie nie stanowią inaczej.

§ 5

1. Przetwarzanie danych osobowych odbywa się w przeznaczonym do tego obszarze, na który składają się pomieszczenia i wydzielone części pomieszczeń opisane w Załączniku nr 1 do Polityki Bezpieczeństwa.
2. Obszar przeznaczony do przetwarzania danych powinien być zabezpieczony w sposób uniemożliwiający dostęp do niego przez osoby nieupoważnione.
3. W przypadku przetwarzania danych osobowych w części pomieszczenia, do którego dostęp mają osoby trzecie, obszar pomieszczenia przeznaczony do przetwarzania danych powinien być wyraźnie wydzielony od pozostałej części pomieszczenia i w sposób uniemożliwiający nieskrępowany dostęp osób trzecich do urządzeń systemu informatycznego.
4. Klucze oraz kody dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych winny być zabezpieczone przed osobami nieupoważnionymi.
5. Udostępnienie kluczy lub kodów dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych osobom nieupoważnionym przez administratora systemu informatycznego lub administratora danych jest zabronione.
6. Osoba nieupoważniona nie może przebywać sama w pomieszczeniu przeznaczonym do przetwarzania danych.
7. Administrator Systemu Informatycznego ponosi odpowiedzialność za właściwe zabezpieczenie kluczy oraz kodów dostępów do pomieszczeń.

§ 6

1. Upoważniona osoba zobowiązana jest do zachowania w tajemnicy swojego loginu i hasła do systemu informatycznego.
2. Upoważniona osoba zobowiązana jest do zachowania w tajemnicy wszelkich informacji pozyskanych w związku z przetwarzaniem danych osobowych.
3. Upoważniona osoba zobowiązana jest do stosownego zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, za każdym razem, kiedy pomieszczenie to opuszcza.
4. Zabrania się podłączania do urządzeń stanowiących część systemu informatycznego służącego do przetwarzania danych nośników danych, które nie zostały przeznaczone do tego celu i które nie zostały sprawdzone pod kątem bezpieczeństwa przy zastosowaniu odpowiednich programów.
5. Upoważniona osoba zobowiązana jest do przetwarzania danych w sposób nie zagrażający ich bezpieczeństwu, w szczególności poprzez stosowanie się do zaleceń administratora systemu informatycznego.
6. Upoważniona osoba ponosi odpowiedzialność za nieuprawnione udostępnienie loginu lub hasła innym osobom, a także za niezabezpieczenie pomieszczenia przeznaczonego do przetwarzania danych osobowych.
7. Ujawnienie przez upoważnioną osobę informacji dotyczących przetwarzanych danych osobowych stanowi poważne naruszenie i może być podstawą do cofnięcia upoważnienia.

§ 7

System informatyczny zabezpieczony jest w szczególności poprzez oprogramowanie antywirusowe, antyszpiegowskie oraz firewall.

1. Zabezpieczenie przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej zapewnione jest poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowywane będą w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwane niezwłocznie po ustaniu ich użyteczności. Kopie zapasowe sporządzane są w 1 egzemplarzu na zewnętrznym nośniku danych.

V. Zbieranie danych i rejestracja zbiorów danych

§ 1

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1. adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2. celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3. źródle danych,
4. prawie dostępu do treści swoich danych oraz ich poprawiania,
5. nazwie podmiotu dla którego zbierane są dane oraz jeżeli dane osobowe będą przetwarzane przez Przetwarzającego oraz informacji o nim wymienionych w pkt 1 -4

§ 2

1. Stosownie do przepisów prawa, „ZUZIK" zobowiązany jest do rejestracji zbiorów danych.
2. „ZUZIK" przygotowuje zgłoszenia rejestracyjne i zgłoszenia aktualizacyjne zbiorów danych.
3. Zgłoszenia dokonują członkowie Zarządu stowarzyszenia zgodnie z obowiązującymi zasadami reprezentacji.
4. Dopóki nie zostaną utworzone trwałe zbiory danych osobowych, „ZUZIK" nie rejestruje ich w ogólnopolskim rejestrze zbiorów danych osobowych prowadzonych przez Generalnego Inspektora Danych Osobowych.

VI. Przetwarzanie danych osobowych i ich udostępnianie

§ 1

1. Dane osobowe przetwarzane są przez upoważnione osoby w sposób zapewniający bezpieczeństwo przetwarzanych danych.
2. Dane osobowe przetwarzane są jedynie w celu, w jakim zostały zgromadzone i jedynie w zakresie niezbędnym dla realizacji tego celu.
3. Wykaz upoważnionych osób wraz z okresem upoważnienia oraz zakresem upoważnienia prowadzi i aktualizuje Administrator Systemu Informatycznego.

§ 2

1. „ZUZIK" upoważnia osobę do przetwarzania danych osobowych.
2. Administrator Systemu Informatycznego przyznaje upoważnionej osobie login i hasło do systemu informatycznego.
3. W przypadku uzasadnionego podejrzenia naruszenia przez upoważnioną osobę przepisów prawa o ochronie danych osobowych lub naruszenia Polityki Bezpieczeństwa, „ZUZIK" niezwłocznie cofa upoważnienie dla tej osoby i pozbawia ją dostępu do danych osobowych do czasu wyjaśnienia zaistniałej sytuacji.
4. W przypadku uzasadnionego podejrzenia naruszenia przez upoważnioną osobę przepisów prawa o ochronie danych osobowych lub naruszenia Polityki Bezpieczeństwa Administrator Systemu Informatycznego niezwłocznie blokuje dostęp upoważnionej osoby do systemu informatycznego i zawiadamia „ZUZIK".

§ 3

1. Dane osobowe udostępniane są na pisemny, umotywowany wniosek, chyba, że przepisy ustawy stanowią inaczej.
2. Osoba rozpatrująca wniosek, o którym mowa w ust. 1, w przypadku jakichkolwiek wątpliwości co do dopuszczalności udostępnienia danych osobowych, przekazuje go „ZUZIK" w celu rozpatrzenia.
3. Zbiory danych, pozyskanych w wyniku świadczenia usług, nie podlegają udostępnieniu osobom trzecim.
4. Obowiązek wskazany w ustępie poprzedzającym nie dotyczy sytuacji, gdy obowiązek udostępnienia tych danych wynika z przepisu prawa.

§ 4

1. Na wniosek osoby, której dane dotyczą, a nie są to dane określone w § 4 ust. 3 „ZUZIK" zobowiązany jest w terminie 30 dni poinformować o przysługujących jej prawach oraz udzielić informacji o których mowa art. 32 ust 1 pkt. 1-5a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, a w szczególności podać w formie zrozumiałej:

   1.1.jakie dane osobowe zawiera zbiór,
   1.2.w jaki sposób zebrano dane,
   1.3.w jakim celu i zakresie dane są przetwarzane,
   1.4.w jakim zakresie oraz komu dane zostały udostępnione.

2. W przypadku jakichkolwiek wątpliwości co do uprawnienia wnioskodawcy, osoba rozpatrująca wniosek przekazuje go „ZUZIK" w celu rozpatrzenia.
3. Na wniosek osoby, której dane dotyczą, informacji udziela się na piśmie.
4. Osoba, której dane dotyczą, ma prawo do uzupełnienia, uaktualnienia, zmiany, usunięcia danych, jeśli dane te są niekompletne, nieaktualne, zbędne dla celu zbierania tych informacji lub jeżeli nie wyraża ona zgody na ich przetwarzanie.

VII. Usuwanie danych osobowych

§ 1

Dane osobowe są przechowywane w sposób uniemożliwiający identyfikację osób, których dotyczą oraz nie dłużej, niż wymaga tego cel, w którym są przetwarzane. Przepisy prawa mogą inaczej określać czas przechowywania danych osobowych.

1. Dane osobowe nie podlegają ewidencjonowaniu poza systemem informatycznym.
2. Decyzję o usunięciu danych lub o zniszczeniu nośników danych podejmuje „ZUZIK"
3. Dane osobowe podlegają usunięciu w obszarze przeznaczonym do przetwarzania danych.
4. Nośniki zawierające dane osobowe oraz informacje o danych osobowych są niszczone w obszarze przeznaczonym do przetwarzania danych pod nadzorem Administratora Systemu Informatycznego. Z czynności tej sporządza się protokół.
5. Na podstawie umowy o powierzenie danych osobowych, dane osobowe oraz nośniki danych osobowych mogą być usuwane i niszczone przez podmiot, któremu powierzono dane osobowe, w sposób uniemożliwiający zapoznanie się z danymi przez osoby nieupoważnione.

VIII. Postanowienia Końcowe

§ 1

1. Niniejsza Polityka powinna być weryfikowana przynajmniej raz do roku przez Zarząd stowarzyszenia i Administratora Systemu Informatycznego lub upoważnioną do tego osobę przez „ZUZIK".
2. Treść Polityki Bezpieczeństwa jest aktualizowana w przypadku wprowadzenia lub zmiany środków technicznych lub organizacyjnych służących ochronie danych

osobowych (zarówno w systemie informatycznym jak i danych przetwarzanych poza tym systemem np. w kartotekach papierowych).

3. Po dokonaniu aktualizacji tworzy się nową wersję Polityki Bezpieczeństwa nadając jej kolejny numer.
4. Zasady Polityki Bezpieczeństwa Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
5. „ZUZIK" jest zobowiązany do zapoznania z treścią Polityki Bezpieczeństwa każdego członka stowarzyszenia.
6. Członek stowarzyszenia zobowiązany jest złożyć oświadczenie, o tym iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi, a także o zobowiązaniu się do ich przestrzegania.
7. W sprawach nieregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy z ustawy z dnia 29 sierpnia 1997r., o ochronie danych osobowych (Dz. U. z 2002r., Nr 101, poz.926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.
8. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa.
9. Polityka wchodzi w życie z dniem jej podpisania.