POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

we Wrocławskim Stowarzyszeniu Abstynentów „STARÓWKA”

I. Zarząd Wrocławskiego Stowarzyszenia Abstynentów „STARÓWKA” świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym, w szczególności prawa osób fizycznych powierzających Stowarzyszeniu swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje:

1. Zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych.
2. Zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w W.S.A. „Starówka” w zakresie problematyki bezpieczeństwa tych danych.
3. Potwierdza traktowanie obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby.
4. Zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

II. Zarząd Wrocławskiego Stowarzyszenia Abstynentów „STARÓWKA” świadomy jest zagrożeń związanych z przetwarzaniem przez Stowarzyszenie danych osobowych na dużą skalę – w tym, w szczególności, z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Jednocześnie Zarząd W.S.A. „Starówka” zamierza doskonalić i rozwijać nowoczesne metody przetwarzania danych.

Zarząd deklaruje, że będzie stale doskonalić i rozwijać organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom:

- związanymi z infekcjami wirusów i koni trojańskich, które instalując się w komputerze mogą wykradać zasoby tego komputera (zarówno stacjonarne jak i sieciowe),
- związanym ze spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera,
- związanych z dostępem do stron internetowych, na części, których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
- związanym z ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera,
- związanym z użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza siedzibą W.S.A. „Starówka”,
- związanym z możliwością niekontrolowanego kopiowania danych na zewnętrzne przenośne nośniki,
- związanych z możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane,
- związanym z lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia,
- związanych z brakiem świadomości niebezpieczeństwa dopuszczania postronnych do swojego stanowiska pracy,
- związanych z atakami z sieci uniemożliwiającymi przetwarzanie (ataki typu Dos na serwer/serwery,
- związanych z działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
- związanych z kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są niezabezpieczone,
- związanych z przekazaniem sprzętu z danymi do serwisu,
- związanych z kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
- związanymi z podszywaniem się przez osoby nieuprawnione pod witrynę internetową, która zbiera dane,

- i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

III. Na podstawie art. 36 ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r.: Dz.U. Nr 101, poz. 926 z późniejszymi zmianami) oraz §3 i §4 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) ustala się następujące wytyczne polityki bezpieczeństwa danych osobowych przetwarzanych we Wrocławskim Stowarzyszeniu Abstynentów „STARÓWKA" w związku z realizacją celów statutowych.

I. POSTANOWIENIA OGÓLNE

Art. 1

1. Dane osobowe w W.S.A. „Starówka" przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   a) Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (teks jednolity z 2002 r.: Dz. U. Nr 101, poz. 926 z późniejszymi zmianami) oraz przepisów wykonawczych z nią związanych.
   b) Przepisów art. 22_1 §1 – 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz. U. Nr 21, poz. 94 z późniejszymi zmianami) i przepisów wykonawczych z nią związanych.
   c) Innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.
2. Dane osobowe w W.S.A. „Starówka" we Wrocławiu przetwarzane są w celu realizacji statutowych celów organizacji. W szczególności dane osobowe przetwarza się:
   a) Dla zabezpieczenia prawidłowego toku realizacji zadań statutowych zgodnie z Ustawą z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie.
   b) W celu zapewnienia prawidłowej, zgodnej z prawem i celami Stowarzyszenia polityki personalnej oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych przez Stowarzyszenie działające jako pracodawca w rozumieniu art.3 kodeksu pracy lub strona innych stosunków zatrudnienia.
   c) Dla realizacji innych usprawiedliwionych celów i zadań W.S.A. „Starówka" we Wrocławiu z poszanowaniem praw i wolności osób powierzających Stowarzyszeniu swoje dane.

Art. 2

Polityka bezpieczeństwa w zakresie ochrony danych osobowych we Wrocławskim Stowarzyszeniu Abstynentów „STARÓWKA" odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1. Tradycyjnych, w szczególności, w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
2. W systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

Art. 3

1. Wrocławskie Stowarzyszenie Abstynentów „STARÓWKA" realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   a) Przetwarzane zgodnie z prawem.
   b) Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   c) Merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane.
   d) Przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Pod szczególną ochroną pozostają wrażliwe dane osobowe wymienione w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym dopuszczalne jest tylko w związku z realizacją celów statutowych Stowarzyszenia i w granicach wynikających z przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Art. 4

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:

1. zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym,
2. zabraniem przez osobę nieuprawnioną,
3. przetwarzaniem z naruszeniem ustawy,
4. zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych.
3. W szczególności Stowarzyszenie zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz innymi zagrożeniami danych , płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

Art. 5

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje kontrole i nadzór nad niszczeniem zbędnych danych osobowych lub ich zbiorów.
2. Niszczenie zbędnych danych osobowych lub ich zbiorów polegać powinno w szczególności na:
   a. Trwałym, fizycznym zniszczeniu danych osobowych lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.
   b. Anonimizacji danych osobowych lub ich zbiorów polegającej na pozbawieniu danych osobowych lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
3. Osoby przetwarzające dane osobowe w Stowarzyszeniu mają obowiązek stosowania oddanych im do dyspozycji narzędzi i technik niszczenia zbędnych danych osobowych lub ich zbiorów.
4. Naruszanie przez zatrudnione w ramach stosunku pracy, osoby upoważnione do dostępu i/lub przetwarzania danych osobowych stosowanych w Stowarzyszeniu procedur niszczenia zbędnych danych osobowych i/lub ich zbiorów traktowane będzie , jako ciężkie naruszenie obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.
5. Kontrola i nadzór nad niszczeniem zbędnych danych osobowych i/lub ich zbiorów może w szczególności polegać na wprowadzeniu odpowiednich procedur niszczenia danych, a także zleceniu niszczenia ich wyspecjalizowanym podmiotom zewnętrznym, gwarantującym bezpieczeństwo procesu niszczenia danych odpowiednie do rodzaju nośnika tych danych.

Art. 6

Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzą w szczególności:

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu.
2. Instrukcja określająca sposób zarządzania i formy zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych we Wrocławskim Stowarzyszeniu Abstynentów „STARÓWKA”.
3. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych we Wrocławskim Stowarzyszeniu Abstynentów „STARÓWKA”.
4. Inne instrukcje, wytyczne i polecenia służbowe określające zasady i procedury mające znaczenie dla ochrony danych osobowych wydawane przez Zarząd Stowarzyszenia oraz upoważnione prze niego osoby.

II. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Art. 7

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych udostępnia przetwarzane na jego obszarze dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych obowiązujących w tym zakresie na jego obszarze.
2. Upoważnienie, którym mowa w art. 7 pkt 1, wynikać może w szczególności:
   a. z charakteru pracy wykonywanej na danym stanowisku,
   b. z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy,

c. z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

Art. 8

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będących dysponentami tych danych.
2. Dysponentami danych osobowych są osoby, które powierzyły swoje dane Stowarzyszeniu w związku z przystąpieniem do stowarzyszenia jako członek, zatrudnienia w Stowarzyszeniu i jednostkach mu podległych, uczestnictwem w projektach realizowanych w Stowarzyszeniu.

Art. 9

1. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, mające interes prawnych lub faktyczny w uzyskaniu dostępu do tych danych mogą mieć wgląd wyłącznie w obecności upoważnionego pracownika Stowarzyszenia po sprawdzeniu uprawnienia do zapoznania się z danymi.
2. Zasada wyrażona w art. 9 ust. 1 ma także zastosowanie do przypadku korzystania przez związki zawodowe z uprawnień przysługujących im na mocy ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz.U.Nr 21, poz. 94 z późniejszymi zmianami) i Ustawy z dnia 23 maja 1991 r. o związkach zawodowych (tekst jednolity z 2001 r.: Dz.U.Nr 79, poz. 854 z późniejszymi zmianami).

Art. 10

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych osobowych lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. W szczególności dostęp do danych osobowych na wskazanej w art. 10 ust. 1 zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, Wojskowe Służy Informacyjne, Sady Powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – wszystkie ww. po okazaniu dokumentów potwierdzających te uprawnienia.

III. OSOBY PRZETWARZAJACE DANE OSOBOWE.

Art. 11

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza osoby odpowiedzialne za bieżącą realizację tej polityki na terenie Stowarzyszenia,a w szczególności:
   a. administrator danych osobowych w rozumieniu art. 7 pkt 4 Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
   b. inne osoby wykonujące zadania ochrony danych osobowych.
2. Wyżej wymienieni wyznaczeni zostają w szczególności w drodze zarządzeń Zarządu Stowarzyszenia.

Art. 12

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dopuszcza do ich przetwarzania w systemie informatycznymi/lub tradycyjnym wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych lub inna upoważnioną do tego osobę.
2. Upoważnienie, o którym mowa w art. 12 pkt 1, wynikać może w szczególności:
   a. z charakteru wykonywanej na danym stanowisku pracy,
   b. z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy,
   c. z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

Art. 13

Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia kontrolę nad dostępem do tych danych. Kontrola ta w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrażanie procedur udzielania dostępu do tych danych.

Art. 14

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zaznajomienie osób upoważnionych do dostępu i/lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Stowarzyszeniu.
2. W szczególności osoby, wskazane w art. 14 ust. 1, zaznajamiane są z kwestiami wymienionymi w tym przepisie przed dopuszczeniem do pracy na stanowiskach związanych z przetwarzaniem danych

osobowych, a także odpowiednio, w trakcie trwania zatrudnienia – w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub technikach i środkach ochrony danych stosowanych w Stowarzyszeniu.

3. Zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Stowarzyszeniu, może odbywać się w szczególności poprzez:
   a. instruktaż na stanowisku pracy,
   b. szkolenie wewnętrzne realizowane na terenie Stowarzyszenia,
   c. szkolenie zewnętrzne.

Art. 15

Osoby upoważnione przez Stowarzyszenie do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą. W szczególności są one informowane o powinności zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stosowanych w Stowarzyszeniu.

Art. 16

Naruszenie przez zatrudnione w ramach stosunku pracy osoby, upoważnione do dostępu i/lub przetwarzania danych osobowych, zasad bezpiecznego i zgodnego z prawem ich przetwarzania, traktowane będzie jako ciężkie naruszenie podstawowych obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

IV. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE PRZEZ STOWARZYSZENIE.

Art. 17

1. Stowarzyszenie zapewnia osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizację uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
2. W szczególności każdej osobie, której dane osobowe są przetwarzane w związku z realizacją celów statutowych Stowarzyszenia, przysługuje prawo do uzyskania informacji o zakresie jego uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzanych danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w art. 32 – 35 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Osoby fizyczne, których dane osobowe są przetwarzane w związku z realizacją celów statutowych Stowarzyszenia, uzyskują informacje o przysługujących im prawach w sposób przyjęty w Stowarzyszeniu.

V. BUDYNKI, POMIESZCZENIA I CZĘŚCI POMIESZCZEŃ, TWORZĄCE OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Art. 18

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych wyznacza budynki, pomieszczenia i części pomieszczeń, tworzące obszar Stowarzyszenia, w którym przetwarzane są dane osobowe.
2. W przypadku, gdy w pomieszczeniu znajduje się cześć ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.
3. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe, może być w szczególności dokonane przez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
4. Pod szczególną ochroną przed niepowołanym dostępem do danych osobowych pozostają urządzenia wchodzące w skład systemu informatycznego Stowarzyszenia w szczególności stacje robocze (poszczególne komputery) wchodzące w skład tego systemu, powinny być umiejscowione w sposób uniemożliwiający osobom nieupoważnionym, bezpośredni i niekontrolowany dostęp do ekranów oraz urządzeń służących do przetwarzania, a zwłaszcza kopiowania danych.
5. Wykaz budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 1** do Polityki Bezpieczeństwa.
6. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Stowarzyszenia, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub

przetwarzania danych osobowych oraz osoby sprawiające nadzór i kontorsję nad bezpieczeństwem przetwarzania tych danych.

7. Osoby nie upoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Stowarzyszenia, w którym przetwarzane są dane osobowe – wyłącznie w obecności upoważnionego pracownika Stowarzyszenia, lub – w razie jego nieobecności – na postawia upoważnienia wydanego, przez administratora danych osobowych lub inną upoważnioną osobę.

Art. 19

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzania danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobowych osobom niepowołanym.
3. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia budynku i/lub pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

Art. 20

1. Dostęp do budynków i pomieszczeń Stowarzyszenia, w których przetwarzane są dane osobowe podlega kontroli.
2. Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia/budynku oraz godzinę pobrania lub zdania klucza.
3. Klucze do budynków i/lib pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do danych budynków, lub pomieszczeń na innych zasadach.
4. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może prowadzić inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.

VI. ZBIORY DANYCH OSOBOWYCH TWORZONE W STOWARZYSZENIU.

Art. 21

1. Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem:
   a. Struktury zbiorów danych,
   b. Programów zastosowanych do przetwarzania tych danych określa **załącznik nr 2** do Polityki Bezpieczeństwa Stowarzyszenia.

Art. 22

Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zgodną z przepisami rozdziału 5 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ochronę zbiorom danych osobowych sporządzonym doraźnie, wyłącznie ze względów technicznych, w związku z projektami realizowanymi w Stowarzyszeniu, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji.

Art. 23

Stowarzyszenie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów statutowych Stowarzyszenia.