Stowarzyszenie
"Europa Iuvenis"
Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788
info@europaiuvenis.org

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Rozdział 1
Postanowienia ogólne

§ 1

Polityka Bezpieczeństwa, zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w organizacji.

§ 2

Użyte w Polityce określenia oznaczają:

1. **Administrator Danych**: organizacja pozarządowa,
2. **Ustawa**: ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
3. **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. Nr 100, poz. 1024),
4. **Użytkownik:** osobę upoważnioną do przetwarzania danych osobowych u administratora,
5. **Administrator Bezpieczeństwa Informacji:** osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych przetwarzanych u Administratora,
6. **Administrator Systemu u Beneficjenta:** osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innej osobie upoważnionej,
7. **Naruszenie zabezpieczenia danych osobowych:** jakiekolwiek naruszenie

bezpieczeństwa, niezawodności, integralności lub poufności zbiorów danych osobowych,

8. **Dane osobowe**: wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
9. **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych,
10. **Usuwanie danych osobowych**: zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
11. **Zbiór danych osobowych** - posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
12. **Zabezpieczenie danych osobowych**: środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą,
13. **Instrukcja** - Instrukcję Zarządzania Systemem Informatycznym,

Rozdział 2
Zakres oraz zasady zabezpieczania danych osobowych

§ 3

1. Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych.
2. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w Polityce oraz Instrukcji, oraz nad wykonywaniem zadań związanych z ochroną danych osobowych u Administratora Danych, sprawuje Administrator Bezpieczeństwa Informacji.

§ 4.

1. Przetwarzanie danych osobowych jest dopuszczalne wyłącznie w zakresie niezbędnym

do udzielenia wsparcia, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli oraz prowadzenia bieżącej działalności organizacji.

2. Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych 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 (dane osobowe wrażliwe).

§ 5.

1. W przypadku zbierania jakichkolwiek danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do otrzymania zgody na przetwarzanie danych osobowych oraz do przekazania tej osobie, informacji o:
   - pełnej nazwie Administratora Danych oraz jego adresie,
   - celu zbierania danych osobowych,
   - prawie dostępu do treści swoich danych osobowych oraz ich poprawiania,
   - dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich
   - przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym przez Administratora Danych,
2. Wzór zgody i informacji stanowi **załącznik nr 1** do niniejszej Polityki.

§ 6.

1. Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.
2. Wnioski o udostępnienie danych osobowych przetwarzanych przez Administratora Danych, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 7.

1. Przetwarzanie danych osobowych znajdujących się w posiadaniu Administratora Danych może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.
2. Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych powinny zostać przed podpisaniem, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Administratora Bezpieczeństwa Informacji.

§ 8.

Każdej osobie, której dane osobowe są przetwarzane, przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych,
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 9.

Na wniosek osoby, której dane osobowe dotyczą, Administrator Danych jest zobowiązany, w terminie maksymalnie 30 dni od dnia wpłynięcia wniosku, wskazać w powszechnie zrozumiałej formie: jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez Administratora

Danych, w jaki sposób zebrano te dane osobowe, w jakim celu i zakresie te dane osobowe są przetwarzane, od kiedy są przetwarzane te dane osobowe, w jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§ 10.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane przez Administratora Danych są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane, Administrator Danych jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

Rozdział 4
Obowiązki Administratora Bezpieczeństwa

§ 11.

1. Administrator Bezpieczeństwa Informacji, poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych u Administratora Danych.
2. Do zadań Administratora Bezpieczeństwa Informacji należy, w szczególności:
   - zgłaszanie zbiorów danych osobowych do Głównego Inspektora Ochrony Danych Osobowych w przypadkach wskazanych w ustawie,
   - prowadzenie i aktualizacja rejestru, o którym mowa w § 19, który stanowi **załącznik nr 2 d**o Polityki,
   - prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który stanowi **załącznik nr 3** do Polityki,
   - analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych oraz pisemne informowanie o wynikach analizy osoby upoważnione

do podejmowania decyzji w imieniu Administratora Danych,

- opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w podmiotowi zewnętrznemu wobec Administratora Danych,
- inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych u Administratora Danych,
- wydawanie i odwoływanie upoważnień do przetwarzania danych osobowych

§ 12.

W doborze i stosowaniu środków ochrony danych osobowych Administrator Bezpieczeństwa Informacji zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 13.

1. Obowiązki Administratora Bezpieczeństwa Informacji wykonywane są przez osobę wyznaczoną.
2. Nadzór nad wykonywaniem obowiązków przez Administratora Bezpieczeństwa Informacji i Administratora Systemu (o ile został powołany), pełni osoba upoważniona do podejmowania decyzji w imieniu Administratora Danych.

Rozdział 5
Przetwarzanie danych osobowych

§ 14.

1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy, współpracownicy, wolontariusze, członkowie organizacji, posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w **załączniku nr 4 do** niniejszej Polityki.
2. Każdy pracownik, współpracownik, wolontariusz, członek organizacji, przed dopuszczeniem do przetwarzania danych osobowych musi być zapoznany z przepisami

dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją. Osoba ta potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji której wzór jest określony w **załączniku nr 5** do niniejszej Polityki.

§ 15.

1. Każda osoba mająca dostęp do danych osobowych, powinna zostać wpisywana do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji
2. Rejestr, o którym mowa w ust. 1, zawiera: imię i nazwisko osoby mającej dostęp, jej identyfikator w systemie informatycznym służącym przetwarzaniu danych, zakres przydzielonego uprawnienia, datę przyznania uprawnień, podpis Administratora Bezpieczeństwa Informacji potwierdzający przyznanie uprawnień, datę odebrania uprawnień, podpis Administratora Bezpieczeństwa Informacji potwierdzający odebranie uprawnień.

§ 16.

1. Dopuszczenie do przetwarzania danych osobowych przez osoby niebędące pracownikami, współpracownikami, wolontariuszami lub członkami organizacji, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych.
2. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 17.

Wszyscy pracownicy, współpracownicy, wolontariusze i członkowie organizacji oraz osoby, o których mowa w § 16 ust. 1, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń

danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 18.

Użytkownicy są, w szczególności, zobowiązani do:

- bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji, określonych w Polityce, Instrukcji i innych procedurach,
- przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach),
- zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania danymi osobowymi,
- niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie,
- nieudzielania informacji o danych osobowych przetwarzanych u Administratora Danych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,
- bezzwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 19.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w **załączniku nr 6 d**o niniejszej Polityki.

Rozdział 6

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 20.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- stwierdzono naruszenie zabezpieczenia,
- stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
- inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych u Administratora Danych.

§ 21.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie: poinformować pisemnie o zaistniałym zdarzeniu Administratora Danych, zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu.
3. Administrator Bezpieczeństwa Informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych jest zobowiązany niezwłocznie:

- wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać,
- przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby niepowołanej do danych osobowych w systemie informatycznym służącym przetwarzaniu danych osobowych,
- podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych, w szczególności przez :

fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej, wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych, zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu,

- szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
- przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych.

§ 22.

1. Po przywróceniu normalnego stanu danych osobowych, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa oraz wewnętrznych uregulowań Administratora Danych, a w przypadku gdy użytkownik nie jest pracownikiem, współpracownikiem, wolontariuszem, członkiem organizacji, konsekwencje wynikające z umowy.

§ 23.

1. Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia danych osobowych i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia danych osobowych przekazuje go Administratorowi Danych.
2. Jeżeli naruszenie zabezpieczenia nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych w Administrator Bezpieczeństwa Informacji przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu u Beneficjenta (o ile został powołany).

Rozdział 7
Kontrola nad przestrzeganiem ochrony danych osobowych

§ 24.

1. Bieżąca kontrola nad przetwarzaniem danych osobowych jest dokonywana przez Administratora Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji przeprowadza raz w roku, kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.
3. Kontrola, o której mowa w punkcie poprzednim, polega w szczególności na sprawdzeniu:
    - którzy pracownicy, współpracownicy, wolontariusze, członkowie organizacji mają dostęp do danych osobowych,
    - czy dane osobowe nie zostały udostępnione nieupoważnionym osobom,
    - czy inne osoby mające dostęp do danych osobowych przetwarzanych u Administratora Danych posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę .

Rozdział 8

Postanowienia końcowe

§ 25.

1. Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych.
2. Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia danych osobowych.
3. Wykazy i rejestry znajdujące się w załącznikach nr 1-8 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji.
4. Integralną część niniejszej Polityki stanowią następujące załączniki:

Załącznik nr 1 wzór zgody na przetwarzanie danych osobowych,

Załącznik nr 2 rejestr osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 3 wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe u Administratora Danych,

Załącznik nr 4 wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych,

Załącznik nr 5 lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych,

Załącznik nr 6 określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych,

Załącznik nr 7 opis struktury zbioru danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

Załącznik nr 8 wykaz zbiorów danych osobowych

Stowarzyszenie
"Europa Iuvenis"
Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788
info@europaiuvenis.org

Załącznik nr 1

do Polityki Bezpieczeństwa

OŚWIADCZENIE WYRAŻENIU ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

W związku z przystąpieniem do Projektu/do bazy wolontariuszy/……(inne –wpisać jakie) wyrażam zgodę na przetwarzanie moich danych osobowych.

Oświadczam, iż przyjmuję do wiadomości, że:

1) Administratorem tak zebranych danych osobowych jest organizacja.....z siedzibą .....

2) Moje dane osobowe będą przetwarzane wyłącznie w celu: .....*udzielenia wsparcia, realizacji projektu ……., ewaluacji, kontroli, monitoringu i sprawozdawczości w ramach, realizacji porozumienia z wolontariuszem……(inne wpisać jakie)*

3) Moje dane osobowe mogą zostać udostępnione innym podmiotom wyłącznie w celu: *udzielenia wsparcia, realizacji projektu ……., ewaluacji, kontroli, monitoringu i sprawozdawczości w ramach ……(inne wpisać jakie?)*

4) Podanie danych jest dobrowolne, aczkolwiek odmowa ich podania jest równoznaczna z brakiem możliwości udzielenia wsparcia w ramach Projektu;

5) Mam prawo dostępu do treści swoich danych i ich poprawiania.

MIEJSCOWOŚĆ I DATA

CZYTELNY PODPIS……

Stowarzyszenie
"Europa Iuvenis"

Damrota 6/4
45-064 Opole

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788

info@europaiuvenis.org

Załącznik nr 2
do Polityki Bezpieczeństwa

Rejestr osób upoważnionych do przetwarzania danych osobowych u Administratora Danych

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis ABI	Data odebrania uprawnień	Podpis Administratora
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

Stowarzyszenie
"Europa Iuvenis"

Damrota 6/4
45-064 Opole

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788

info@europaiuvenis.org

Załącznik nr 3
do Polityki Bezpieczeństwa

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe u Administratora Danych

Lp.	Budynek – dane adresowe	Pomieszczenie

Stowarzyszenie "Europa Iuvenis"
Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788
info@europaiuvenis.org

Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE Nr .....DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ……r., na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), upoważniam ……do przetwarzania danych osobowych w organizacji …….. Upoważnienie obowiązuje do dnia odwołania. Upoważnienie wygasa z chwilą ustania Pana/Pani* *zatrudnienia, współpracy, wolontariatu, członkostwa w organizacji.*

……
Czytelny podpis osoby reprezentującej organizację

- niepotrzebne skreślić

ODWOŁANIE UPOWAŻNIENIE Nr ……. z dnia……DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem …… r., na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), odwołuję wydane ……upoważnienie do przetwarzania danych osobowych w organizacji.

……
Czytelny podpis osoby reprezentującej organizację
* niepotrzebne skreślić

Stowarzyszenie
"Europa Iuvenis"

Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788

info@europaiuvenis.org

Załącznik nr 5
do Polityki Bezpieczeństwa

Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, iż zapoznałem/am się z:

- przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)

oraz przepisami wykonawczymi do niniejszej ustawy,

- Polityką Bezpieczeństwa oraz z Instrukcją Zarządzania Systemem Informatycznym

	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1			
2			
3			
4			
5			
6			
7			

Stowarzyszenie
"Europa Iuvenis"
Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788
info@europaiuvenis.org

Załącznik nr 6

do Polityki Bezpieczeństwa

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych

I. Środki ochrony fizycznej danych:

a) klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym,

b) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,

c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

d) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych,

e) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie,

f) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie,

g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

a) Sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby.

b) Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie.

c) Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

d) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

e) Zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III Środki organizacyjne:

a) Osoby uprawione do przetwarzania danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

b) Osoby uprawione do przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.

c) Monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

d) Kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe są przetwarzane na bieżąco.

Stowarzyszenie
"Europa Iuvenis"

Damrota 6/4
45-064 Opole

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788

info@europaiuvenis.org

Załącznik nr 7
do Polityki Bezpieczeństwa

Opis struktury zbioru danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

BAZA 1 : dane osobowe pracowników i współpracowników (zakres : imię, nazwisko, data i miejsce urodzenia, imiona rodziców, adres, PESEL, e-mail, telefon, badania lekarskie, nr konta bankowego) oraz kopie bezpieczeństwa tych danych,

BAZA 2 : dane osobowe uczestników projektów (zakres : imię, nazwisko, adres, PESEL, e-mail, telefon i inne o ile są wymagane przez grantodawców)

BAZA 3 : dane osobowe sponsorów (zakres : imię, nazwisko, adres, PESEL, NIP, e-mail, telefon, nr konta bankowego)

BAZA 4 : dane osobowe członków stowarzyszenia (zakres : imię, nazwisko, adres, PESEL, e-mail, telefon, nr dokumentu tożsamości)

BAZA 5 : dane osobowe członków władz organizacji (zakres : imię, nazwisko, adres, PESEL, e-mail, telefon, nr dokumentu tożsamości)

BAZA 6 : dane osobowe wolontariuszy (zakres : imię, nazwisko, adres, PESEL, e-mail, telefon, nr konta bankowego, nr dokumentu tożsamości)

BAZA 7 : dokumenty finansowe (zakres : imię, nazwisko, nazwa, adres, NIP, PESEL, nr konta bankowego)

BAZA 8 : archiwum

Stowarzyszenie
"Europa Iuvenis"
Damrota 6/4
45-064 Opole

EUROPA IUVENIS

KRS: 0000506238
NIP: 754-308-53-52
REGON: 161610788
info@europaiuvenis.org

Załącznik nr 8
do Polityki Bezpieczeństwa

Wykaz zbiorów danych osobowych

Legenda:
(1) nazwa zwyczajowa lub własna, np.: dane kadrowe, dane płacowe, Dokumentacja ZFŚS, baza klientów stałych
(2) np.: Windows , SQL, Oracle, dokumenty papierowe
(3) np.; (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie transmisji danych, (F) wydzielona fizycznie sieć
(4) (S) – serwer, (K) – miejsce przechowywania kopii bezpieczeństwa, (Z) – pomieszczenie, w którym wykonywane są kopie bezpieczeństwa, (U) – pomieszczenie osób przetwarzających dane, (A) – pomieszczenie administratora bazy danych
(5) (K) – kraty w oknach, (A) – alarm, (W) – wzmocnienie drzwi, (S) – szafa zamykana na klucz, (P) – pomieszczenie zamykane na klucz

Lp.	Nazwa zbioru danych (1)	Forma danych/baza danych (2)	Zabezpieczenie informatyczne (3)	Bazę chroni UPS Tak/nie	Program służący do przetwarzania baz danych	Lokalizacja (adres)	Funkcja lokalizacji (4)	Zabezpieczenie fizyczne (5)
1.	Dane pracowników i współpracowników	Dok. Papierowe, elektroniczne	I	nie				
2.	Dane uczestników projektów	Dok. Papierowe, elektroniczne	I	nie				
3.	Dane osobowe sponsorów	Dok. Papierowe, elektroniczne	I	nie				
4.	Dane osobowe członków stowarzyszenia	Dok. Papierowe, elektroniczne	I	nie				
5.	Dane osobowe członków władz organizacji	Dok. Papierowe, elektroniczne	I	nie				
6.	Dane osobowe wolontariuszy	Dok. Papierowe, elektroniczne	I	nie				
7.	Dokumenty finansowe	Dok. Papierowe, elektroniczne	I	nie				
8.	Archiwum	Dok. papierowe	n/d	nie				