Polityka bezpieczeństwa Międzynarodowego Stowarzyszenia Studentów Medycyny IFMSA-Poland

Zatwierdzona podczas Zgromadzenia Delegatów
w Legnicy, 26 marca 2010 r.

Przyjęta w głosowaniu Zarządu Głównego
dnia 30 sierpnia 2010 r.

Spis treści Polityki bezpieczeństwa IFMSA-Poland:

Preambuła

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity) oraz rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) nakłada na administratora danych osobowych następujące obowiązki:
- zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- zabezpieczenie danych przed nieuprawnionym dostępem,
- zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
- zabezpieczenie przed utratą danych,
- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.
Polityka bezpieczeństwa określa, zgodnie z brzmieniem § 1 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. z 2004 r. Nr 100, poz. 1024), sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Podstawa prawna

Podstawę prawną dla niniejszych regulacji stanowią:

a) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity),
b) 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. z 2004 r. Nr 100, poz. 1024),
c) inne powszechnie obowiązujące przepisy prawa.

Rozdział 1
Regulacje Ogólne

1.1 Zagadnienia wstępne i definicje

1.1.1 Ilekroć w dokumencie mowa o:

a) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity),
b) rozporządzeniu – rozumie się przez to 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. z 2004 r. Nr 100, poz. 1024)
c) IFMSA-Poland – rozumie się przez to Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland,
d) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne bez nadmiernych nakładów finansowych, czasowych lub działań,
e) 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,
f) bezpieczeństwie – rozumie się przez to stan faktyczny uniemożliwiający wykorzystanie, przepływ, modyfikację lub zniszczenie informacji w IFMSA-Poland przez osoby postronne lub nieupoważnione.

1.1.2 Międzynarodowe Stowarzyszenie Studentów Medycyny IFMSA-Poland dokłada wszelkich starań celem zapewnienia bezpieczeństwa informacji w Stowarzyszeniu. W szczególności zapewnia, aby dane były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z prawem celów,
c) merytorycznie poprawne i adekwatne w stosunku do celów,
d) przechowywane (tak żeby ich nie udostępniać i nie przechowywać dłużej niż to konieczne dla osiągnięcia celów).

1.1.3 Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

a) zbierane są dane osobowe,
b) przetwarzane są dane osobowe,
c) dochodzi do kontroli przetwarzania danych osobowych,
d) stwierdzono zagrożenie bezpieczeństwa danych osobowych,
e) stwierdzono naruszenie zabezpieczenia systemu informatycznego.

1.1.4 IFMSA-Poland gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizacje uprawnień gwarantowanych im przez obowiązujące przepisy prawa.

1.1.5 W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacja celów statutowych, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania 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.

1.1.6 Osoby fizyczne, których dane osobowe są przetwarzane w związku z realizacja celów statutowych, uzyskują informacje o przysługujących im prawach w sposób określony w niniejszym dokumencie.

1.2 Administrator danych

1.2.1 Zgodnie z art. 7 pkt 4 ustawy, administratorem danych osobowych jest Zarząd Główny Międzynarodowego Stowarzyszenia Studentów Medycyny IFMSA-Poland z siedzibą w Warszawie, 02-007, ulica Oczki 1a.

1.2.2 Podmiot zwany jest dalej Zarządem Głównym Stowarzyszenia.

1.2.3 Zarząd Główny odpowiedzialny jest za realizację zapisów Polityki bezpieczeństwa IFMSA-Poland i jej przestrzeganie.

1.2.4 Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

1.2.5 Na Administratorze danych ciążą obowiązki wynikające z zapisów ustawy i rozporządzenia.

1.3 Administrator bezpieczeństwa informacji

1.3.1 IFMSA-Poland wyznacza zgodnie z art. 36 ust. 3 ustawy, administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 ustawy.

1.3.2 Administratorem bezpieczeństwa informacji w IFMSA-Poland są członkowie Zarządu Głównego Stowarzyszenia wymienieni w ewidencji osób wchodzących w skład podmiotu Administratora bezpieczeństwa informacji.

1.3.3 Ewidencja, o której mowa w punkcie 1.3.2 prowadzona jest przez Sekretarza Generalnego IFMSA-Poland na podstawie aktualnego składu osobowego Zarządu Głównego zatwierdzonego przez Zgromadzenie Delegatów IFMSA-Poland i stanowi załącznik do niniejszego dokumentu.

1.3.4 Ewidencja, o której mowa w punkcie 1.3.2 zawiera:

a) funkcję osoby upoważnionej,
b) imię i nazwisko osoby,
c) identyfikator, jeśli osoba przetwarza dane w systemie informatycznym,
d) podpis osoby stwierdzającej nadanie uprawnień.

1.3.5 W ramach realizacji swoich obowiązków Zarząd Główny IFMSA-Poland może w drodze uchwały, zgodnie z obowiązującym prawem, wyznaczyć kolejnych administratorów bezpieczeństwa informacji.

1.3.6 Każdorazowo Zarząd Główny określa w uchwale zakres obowiązków i odpowiedzialności dodatkowego administratora bezpieczeństwa informacji.

1.3.7 Administratorzy bezpieczeństwa informacji nie będący członkami Zarządu Głównego wymieniani są w ewidencji osób wchodzących w skład podmiotu Administratora bezpieczeństwa informacji.

1.4 Instrukcja zarządzania systemem informatycznym

1.4.1 Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IFMSA-Poland, o której mowa w § 3 ust. 1 rozporządzenia, zwaną dalej instrukcją - określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych osobowych.

1.4.2 Instrukcja przyjmowana jest w drodze uchwały przez Zarząd Główny IFMSA-Poland i stanowi załącznik do niniejszego dokumentu.

1.4.3 Wszelkie zmiany w instrukcji przyjmowane są w drodze uchwały przez Zarząd Główny IFMSA-Poland, w porozumieniu z pozostałymi administratorami bezpieczeństwa informacji.

1.5 Zbieranie danych osobowych

1.5.1 Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.

1.5.2 W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

a) adresie swojej siedziby i pełnej nazwie,

b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
c) prawie dostępu do treści swoich danych oraz ich poprawiania,
d) dobrowolności podania danych.

1.5.3 Informacja, o której mowa w punkcie 1.5.2 udzielana jest pisemnie najpóźniej w momencie zbierania danych osobowych.

1.6 Udostępnianie danych osobowych

1.6.1 Dane osobowe będące w posiadaniu IFMSA-Poland są udostępniane zgodnie z zapisami ustawy.

1.6.2 Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych , zgodnie z brzmieniem ustawy.

1.6.3 W szczególności administrator danych jest obowiązany, na wniosek osoby, której dotyczą dane, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, w szczególności podać w formie zrozumiałej:
a) jakie dane osobowe zawiera zbiór,
b) w jaki sposób zebrano dane,
c) w jakim celu i zakresie dane są przetwarzane,
d) w jakim zakresie oraz komu dane zostały udostępnione.

1.6.4 Na wniosek osoby, której dane dotyczą, informacji, o których mowa w punkcie 1.5.3 udziela się na piśmie.

1.6.5 IFMSA-Poland może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

1.6.6 Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w ustawie.

Rozdział 2
Wykazy

2.1 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

2.1.1 Dane osobowe przetwarzane są w siedzibie IFMSA-Poland oraz w siedzibach Oddziałów IFMSA-Poland.

2.1.2 Adresy siedzib Oddziałów:

Oddział Białystok	ul. Akademicka 3, 15-267 Białystok
Oddział Bydgoszcz	ul. Jagiellońska 15 lok. 013B, 85-067 Bydgoszcz
Oddział Gdańsk	ul. Dębowa 7 pok. 2, 80-204 Gdańsk
Oddział Kraków	ul. Św. Łazarza 16 pok. 001, 31-530 Kraków
Oddział Lublin	ul. Chodźki 9, 20-093 Lublin
Oddział Łódź	ul. Rodz. Fibaków 2 pok. 134, 90-927 Łódź
Oddział Poznań	ul. Rokietnicka 6 pok. 29/30 60-806 Poznań
Oddział Szczecin	ul. Dunikowskiego 2, 70-123 Szczecin

Oddział Śląsk	ul. Medyków 26 pok. 8 40-752 Katowice
Oddział Warszawa	ul. Oczki 1A, 02-007 Warszawa
Oddział Wrocław	ul. J. Mikulicza Radeckiego 5, 50-368 Wrocław

2.1.3 Pomieszczenia zabezpieczone są przed dostępem osób trzecich.

2.1.4 IFMSA-Poland do przechowywania i przetwarzania danych osobowych korzysta z serwerów oferowanych przez Przedsiębiorstwo VEL.PL, ul. Wiejska 19, 39-400 Tarnobrzeg oraz Az.pl Albert Jerka, Andrzej Kostrzewa Spółka Jawna, ul. Sosnowa 6a, 71-468 Szczecin.

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

2.1.6 Nośniki informacji są przechowywane w siedzibie IFMSA-Poland lub w siedzibach Oddziałów IFMSA-Poland.

2.2 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

2.2.1 Dane osobowe przechowywane są i przetwarzane w formie dokumentów fizycznych, przy użyciu oprogramowania komputerowego oraz systemów wykorzystujących oprogramowanie internetowe.

2.2.2 Istnieją następujące fizyczne zbiory danych osobowych:

a) zbiór deklaracji członkowskich IFMSA-Poland – o wzorze ustalonym przez Zarząd Główny na drodze uchwał wymienionych w załączonym do niniejszego dokumentu załączniku Spis uchwał – przechowywany w Oddziale macierzystym członka IFMSA-Poland lub w siedzibie IFMSA-Poland;
b) zbiór dokumentów wymiany programów SCOPE/SCORE o wzorach ustalonych przez Zarząd Główny IFMSA-Poland na drodze uchwał wymienionych w załączniku Spis uchwał – przechowywany w Oddziale macierzystym członka IFMSA-Poland lub w siedzibie IFMSA-Poland;
c) historia wydarzeń, służąca ocenie aktywności członków IFMSA-Poland – przechowywana w Oddziale macierzystym członka IFMSA-Poland;
d) zbiór uchwał organów Stowarzyszenia przechowywany w siedzibie organu lub w siedzibie IFMSA-Poland;
e) zbiór kwestionariuszy dla kandydatów na Członków Honorowych, Koordynatorów Narodowych, członków Zarządu Głównego, członków Komisji Rewizyjnej przechowywany w siedzibie IFMSA-Poland,
f) zbiór kart transakcji prowadzonych przez osoby odpowiedzialne zgodnie z brzmieniem Procedury przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu IFMSA-Poland.

2.2.3 Dane osobowe przechowywane i przetwarzane są także przy wykorzystaniu platformy systemowej Windows (w wersjach 98, 2000, XP, Vista, 7) oraz platformy Linux.

2.2.4 Dane osobowe przechowywane i przetwarzane są z wykorzystaniem oprogramowania Office w wersjach 97, 2000, 2003, 2007 (w zależności od posiadanej licencji), OpenOffice w wersjach 2 oraz 3.

2.2.5 W każdym wypadku korzystania z systemów i oprogramowania wymienionych w punkcie 2.2.3 i 2.2.4 dostęp do danych chroniony jest według procedur opisanych w rozdziale 5 niniejszego dokumentu.

2.2.6 Dane osobowe przechowywane i przetwarzane są przy użyciu oprogramowania Joomla w wersji nie niższej niż 1.5.0 oraz własnego systemu Intranet IFMSA-Poland na serwerach wymienionych w punkcie 2.1.4.

2.2.7 W każdym wypadku korzystania z internetowych systemów przetwarzania danych wymienionych w punkcie 2.2.6, dostęp do danych chroniony jest według procedur opisanych w rozdziale 5 niniejszego dokumentu.

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

2.3.1 Dane osobowe pochodzące z deklaracji członkowskiej są przetwarzane według następujących pozycji:
a) nazwisko, imię, drugie imię,
b) data urodzenia, miejsce urodzenia,
c) adres zamieszkania, adres korespondencyjny,
d) telefon, e-mail,
e) wydział/kierunek studiów,
f) numer legitymacji, rok studiów, grupa dziekańska,
e) pola wypełniane przez Zarząd Oddziału, w szczególności dotyczące nadania, przedłużenia i wygaśnięcia/utraty członkostwa.

2.3.2 Dane osobowe pochodzące z dokumentów wymiany SCOPE/SCORE/SCORA są przetwarzane według następujących pozycji:
a) nazwisko, imię, drugie imię,
b) data urodzenia, miejsce urodzenia,
c) adres zamieszkania, adres korespondencyjny,
d) telefon, e-mail,
e) numer paszportu, numer dowodu osobistego,
f) wydział/kierunek studiów,
g) numer legitymacji, rok studiów, grupa dziekańska,
h) dane państw, których dotyczy kwalifikacja.

2.3.3 Za dane osobowe przetwarzane bezpośrednio w bazach informatycznych Federacji IFMSA oraz za dane przekazane w procesie kwalifikacji stronie przyjmującej studenta, IFMSA-Poland nie bierze odpowiedzialności, pod warunkiem uprzedniego poinformowania osoby, której dane te dotyczą, o fakcie ich przekazania oraz uzyskania jej zgodą.

2.3.4 Do przekazania danych osobowych w trybie przywołanym w punkcie 2.3.3 dochodzi wyłącznie, gdy przekazanie jest niezbędne do wykonania umowy między administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie, a także spełnione są wymogi art. 47 § 1. ustawy.

2.3.5 Dane osobowe pochodzące z kwestionariuszy kandydatów na członków Zarządu Głównego, członków Komisji Rewizyjnej oraz Koordynatorów Narodowych są przetwarzane według następujących pozycji:
a) funkcja,
b) nazwisko, imię, drugie imię, numer PESEL,
c) data urodzenia, miejsce urodzenia,
d) adres zamieszkania, adres korespondencyjny,
e) telefon, e-mail,
f) wydział/kierunek studiów, uczelnia,
g) numer legitymacji, rok studiów, grupa dziekańska,
h) Oddział zgłaszający, data wstąpienia do IFMSA-Poland,
i) pełnione funkcje w IFMSA-Poland wraz z datami.

2.3.6 Dane osobowe pochodzące z kwestionariusza kandydata na Członka Honorowego są przetwarzane według następujących pozycji:
a) nazwisko, imię, drugie imię, numer PESEL,
b) data urodzenia, miejsce urodzenia,
c) adres zamieszkania, adres korespondencyjny,
d) telefon, e-mail,
e) data wstąpienia do IFMSA-Poland, data ukończenia studiów,
f) dane zgłaszającego,
g) pełnione funkcje w IFMSA-Poland wraz z datami,

h) Oddziały popierające kandydaturę,
i) pola z przebiegu procesu przyznawania członkostwa.

2.3.7 Za zgodność ze stanem faktycznym i poprawność danych kandydata na Członka Honorowego wymienionych w punkcie 2.2.5 odpowiada zgłaszający.

2.3.8 Dane osobowe pochodzące z historii wydarzeń, służącej ocenie aktywności członków IFMSA-Poland są przetwarzane według następujących pozycji:
a) nazwisko, imię, drugie imię,
b) numer deklaracji członkowskiej
c) telefon, e-mail,
d) data wstąpienia do IFMSA-Poland,
e) aktywność członka IFMSA-Poland, udział w wydarzeniach, pełnione funkcje.

2.3.9 Każda uchwała organu IFMSA-Poland zawierająca w swojej treści dane osobowe członka IFMSA-Poland przechowywana i przetwarzana jest zgodnie z zasadami przetwarzania zbiorów danych osobowych.

2.3.10 Dane osobowe pochodzące z kart transakcji, o których mówi Procedura przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu IFMSA-Poland, przetwarzane są według następujących pozycji:
a) nazwisko, imię, drugie imię,
b) obywatelstwo
c) adres,
d) PESEL,
e) data urodzenia,
f) seria i numer paszportu,
g) dane z rejestru wyciągu sądowego (nazwa, forma organizacyjna, siedziba, NIP, dane osób reprezentujących).

Rozdział 3
Osoby przetwarzające dane osobowe

3.1 Osoby upoważnione do przetwarzania danych osobowych

3.1.1 Do przetwarzania wszystkich danych osobowych w obrębie IFMSA-Poland upoważniony jest Zarząd Główny IFMSA-Poland w ramach realizacji swoich zadań statutowych oraz Komisja Rewizyjna IFMSA-Poland w ramach realizacji swoich zadań statutowych.

3.1.2 Do przetwarzania wszystkich danych osobowych dotyczących członków danego Oddziału upoważnieni są: Prezydent, Sekretarz oraz Skarbnik tego Oddziału oraz członkowie Komisji Rewizyjnej Oddziału.

3.1.3 Do przetwarzania danych osobowych członków danego Oddziału w zakresie ich aktywności upoważnieni są członkowie Zarządu tego Oddziału.

3.1.4 Do przetwarzania danych osobowych w zakresie niezbędnym do realizacji procesu rekrutacji i nadzoru wymian SCOPE/SCORE/SCORA w IFMSA-Poland upoważnione są osoby wymienione w punkcie 3.1.2 oraz odpowiednio LEO/LORE w obrębie danych dotyczących członków macierzystego Oddziału oraz studentów przyjeżdżających do tego Oddziału, zaś NEO/NORE/NORA w obrębie danych członków IFMSA-Poland i Federacji IFMSA.

3.1.5 Do przetwarzania danych osobowych członków IFMSA-Poland w zakresie ich aktywności w Programach Stałych upoważnieni są Koordynatorzy Narodowi Programów Stałych, w zakresie właściwym dla działalności ich Programu Stałego.

3.1.6 Do przetwarzania danych osobowych członków IFMSA-Poland w zakresie ich aktywności w Projektach Ogólnopolskich upoważnieni są Koordynatorzy Ogólnopolskich Projektów, w zakresie wymienionym w uchwale powołującej stanowisko Koordynatora.

3.1.7 Do przetwarzania danych osobowych członków IFMSA-Poland Alumni uprawniony jest Koordynator IFMSA-Poland Alumni.

3.1.8 Do przetwarzania danych osobowych członków Zespołów IFMSA-Poland uprawniony jest Koordynator Zespołu, w zakresie niezbędnym dla realizacji zadań tego Zespołu.

3.1.9 Do przetwarzania danych pochodzących z kart transakcji, o których mówi Procedura przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu IFMSA-Poland uprawnione jest Skarbnik IFMSA-Poland, Wiceprezydent IFMSA-Poland ds. marketingu, pozostali Członkowie Zarządu Głównego oraz członkowie Komisji Rewizyjnej w ramach ich czynności statutowych.

3.1.10 Uprawnienia, których zakres wymieniają punkty od 3.1.1 do 3.1.8, nadawane są poprzez automatyczne naniesienie danych osoby upoważnionej do przetwarzania danych osobowych do Ewidencji, zgodnie z bazą teleadresową Wiceprezydenta IFMSA-Poland ds. zasobów ludzkich oraz poprzez przesłanie Upoważnienia do przetwarzania danych osobowych, którego kopię osoba ta winna podpisać i złożyć we właściwym archiwum IFMSA-Poland.

3.1.11 Osoby będące Asystentami w rozumieniu Regulaminu IFMSA-Poland uzyskują uprawnienia do przetwarzania danych osobowych w zakresie określonym przez osobę powołującą, lecz nie przekraczających uprawnień tej osoby.

3.1.12 Asystent uzyskuje wyżej wymienione uprawnienia w chwili dodania jego danych do Ewidencji. Dane przekazywane są Sekretarzowi Generalnemu przez osobę powołującą dla osób pełniących funkcje ogólnopolskie, zaś w przypadku funkcji lokalnych dane asystenta przekazywane są za pośrednictwem Sekretarza Oddziału.

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

3.1.14 Za datę wygaśnięcia uprawnień przyjmuje się datę końca pełnienia funkcji, na którą osoba ta została wybrana, zaś w przypadku Asystenta datę końca pełnienia funkcji przez osobę powołującą.

3.2 Nadawanie dodatkowych uprawnień

3.2.1 Zarząd Główny w drodze uchwały może nadać uprawnienia do administrowania danymi osobowymi w obrębie IFMSA-Poland osobom niewymienionym w punkcie 3.1 lub może rozszerzyć ich uprawnienia.

3.2.2 Każdorazowo Zarząd Główny określa w wyżej wymienionej uchwale funkcję osoby upoważnionej, imię i nazwisko, datę nadania i wygaśnięcia uprawnień, zakres upoważnienia oraz uzasadnienie nadania uprawnień lub ich rozszerzenia. Dane te odnotowywane są również w Ewidencji osób przetwarzających dane osobowe.

3.3 Ewidencja osób przetwarzających dane osobowe

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

3.3.2 Ewidencja zawiera:

a) funkcję osoby upoważnionej,
b) imię i nazwisko osoby upoważnionej,
c) datę nadania i datę ustania upoważnienia,
d) zakres upoważnienia do przetwarzania danych osobowych,
e) identyfikator, jeśli osoba przetwarza dane w systemie informatycznym,
f) podpis osoby stwierdzającej nadanie uprawnień.

3.3.3 Ewidencja prowadzona jest przez Administratora danych osobowych, a w szczególności za jej prowadzenie odpowiada Sekretarz Generalny IFMSA-Poland czyniąc to na podstawie aktualnej bazy teleadresowej sporządzanej przez Wiceprezydenta IFMSA-Poland ds. zasobów ludzkich

zgodnie z punktem 11.2.2.b Regulaminu IFMSA-Poland oraz zgodnie z uchwałami Zarządu Głównego i decyzjami Prezydenta Oddziału, we wskazanym uprzednio zakresie.

3.4 Obowiązki osoby przetwarzającej dane

3.4.1 Każda osoba uprawniona do przetwarzania danych osobowych w IFMSA-Poland w jakimkolwiek zakresie zobowiązana jest zapoznać się z Polityką bezpieczeństwa IFMSA-Poland oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i postępować zgodnie z nimi.

3.4.2 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.

3.4.3 Każda osoba przetwarzająca dane zobowiązana jest, niezwłocznie po objęciu przez nią funkcji, a przed przystąpieniem do przetwarzania danych osobowych, podpisać kopię Upoważnienia do przetwarzania danych osobowych w IFMSA-Poland, które stanowi załącznik do niniejszego dokumentu.

3.4.4 Treść Upoważnienia, o którym mowa w punkcie 3.4.3, uchwalana jest przez Zarząd Główny IFMSA-Poland.

3.4.5 Upoważnienie, o którym mowa w punkcie 3.4.3, przechowywane jest w Archiwum IFMSA-Poland: Oddziałowym dla członków Zarządów Oddziałów i osób wyznaczonych przez Prezydenta Oddziału lub centralnym dla pozostałych osób.

Rozdział 4
Przepływ danych

4.1 Sposób przepływu danych pomiędzy poszczególnymi systemami

4.1.1 Administrator dopuszcza przepływ danych między poszczególnymi systemami.

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

4.1.3 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 2.2.2 niniejszego dokumentu.

4.1.4 Za przetwarzanie danych zebranych w formie, o jakiej mówi punkt 4.1.3, odpowiada osoba upoważniona do przetwarzania tych danych osobowych, w zakresie upoważnienia.

4.1.5 Każdorazowo o powstaniu dokumentów, o których mówi punkt 4.1.3, informowany jest w formie pisemnej przez osobę tworzącą dokument Sekretarz Generalny IFMSA-Poland. Prowadzi on spis tych dokumentów wraz z określeniem osób upoważnionych do ich przetwarzania.

4.1.6 Dane mogą być wprowadzane i wymieniane w obrębie systemu Intranet IFMSA-Poland na zasadach określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IFMSA-Poland.

Rozdział 5
Środki techniczne zapewniające poufność danych

5.1 Zagadnienia wstępne

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

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

5.2 Fizyczne zbiory danych

5.2.1 Fizyczny zbiór danych osobowych przechowywany jest w formie uporządkowanej sygnaturami dokumentów. Dla deklaracji członkowskich zamiast numeru sygnatury stosuje się numer deklaracji.

5.2.2 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 2.1.2.

5.2.3 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.

5.3 Elektroniczne zbiory danych

5.3.1 Przez elektroniczne zbiory danych rozumie się zbiory wymienione w punktach 4.1.2 i 4.1.3, przetwarzane w sposób wymieniony w punktach 2.2.3 i 2.2.4 Polityki bezpieczeństwa IFMSA-Poland.

5.3.2 Dokumenty przetwarzane są na urządzeniach znajdujących się w pomieszczeniach, o których mówi punkt 2.1.2.

5.3.3 Urządzenia powyższe zabezpieczone są przed kradzieżą.

5.3.4 Bezpośredni dostęp do danych jest zabezpieczony.

5.3.5 Zabezpieczenie, o którym mowa w punkcie 5.3.4 realizowane jest poprzez:

a) utworzenie osobnych kont dla użytkowników w systemach, o których mowa w punkcie 2.2.3 niniejszego dokumentu,
b) zabezpieczenia hasłem dostępu do plików przy użyciu programów, o których mowa w punkcie 2.2.4 niniejszego dokumentu,
c) zabezpieczenie folderu, w którym przechowywane są dane, hasłem - jeśli żadne z powyższych jest niemożliwe.

5.3.6 Zabezpieczenie, o którym mowa w punkcie 5.3.5.a polega na utworzeniu nazwy użytkownika i hasła. Są one indywidualne dla każdej osoby uprawnionej do przetwarzania danych.

5.3.7 Przez hasło rozumie się minimum 8-znakową kombinację cyfr i liter, zgodną z postanowieniami ustawy i aktów wykonawczych.

5.3.8 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 zewnętrzna.

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

5.3.10 Na osobie uprawnionej do przetwarzania danych osobowych spoczywa obowiązek dbania o aktualizacje oprogramowania wymienionego

w punktach 5.3.8 i 5.3.9, a także samego systemu i oprogramowania, wymienionych w punktach 2.2.3 i 2.2.4.

5.3.11 Wszelkie nośniki danych znajdują się w pomieszczeniach wskazanych w punkcie 2.1.2 i są zabezpieczone przed ich wyniesieniem bądź zniszczeniem przez nieuprawnione osoby.

5.3.12 Dostęp do danych zgromadzonych na nośnikach, w szczególności nośnikach służących zapisywaniu kopii zapasowych, tj. płyt CD, DVD, dyskietek, urządzeń typu pendrive, dysków wymiennych, winien być zabezpieczony hasłem.

5.3.13 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.

5.4 Zbiory danych w systemach Intranet i Joomla

5.4.1 Zbiór danych osobowych w systemie Intranet i na platformie Joomla chroniony jest z wykorzystaniem nowoczesnych mechanizmów szyfrowania.

5.4.2 Administrator bezpieczeństwa informacji odpowiada za wszelkie aktualizacje systemu poprawiające jego bezpieczeństwo.

5.4.3 Szczegółowy opis zabezpieczeń i uwierzytelniania dostępu zawiera Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IFMSA-Poland.

5.5 Kopie zapasowe

5.5.1 Za sporządzenie kopii zapasowej danych odpowiada osoba bezpośrednio administrująca tymi danymi. Sposoby tworzenia kopii zapasowych w systemach Intranet i Joomla określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IFMSA-Poland.

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

5.5.3 Kopia zapasowa danych przechowywana jest na nośniku zewnętrznym, ze szczególnym uwzględnieniem punktów 5.3.11 i 5.3.12 niniejszego dokumentu.

5.5.4 Osoba administrująca zbiorem danych osobowych tworzy kopie zapasowe tego zbioru za ostatnie 12 miesięcy oraz przechowuje je w pomieszczeniach wskazanych w punkcie 2.1.2.

5.6 Przekazywanie danych

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

5.6.2 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 IFMSA-Poland.

5.6.3 Jeśli brak jest następcy, osoba, o której mowa w punkcie 5.6.2 przekazuje zbiory danych i ich kopie przewodniczącemu organu IFMSA-Poland, którego jest członkiem lub swojemu bezpośredniemu zwierzchnikowi.

5.6.4 Jeśli przekazanie zbiorów danych jest mimo to nadal niemożliwe, także zgodnie z punktem 5.6.3, osoba tracąca prawo do przetwarzania danych osobowych zobowiązana jest przekazać te dane i ich kopie Sekretarzowi Generalnemu IFMSA-Poland.

5.6.5 Osoba, o której mowa w punkcie 5.6.2, przekazuje także zgodnie z procedurą wymienioną powyżej wszelkie loginy i hasła umożliwiające dostęp do danych osobowych.

5.6.6 Posiadanie lub przetwarzanie danych osobowych należących do IFMSA-Poland przez osoby, które nie posiadają do tego uprawnień jest sprzeczne z polskim prawem.

5.7 Przenoszenie danych

5.7.1 Możliwe jest przenoszenie danych osobowych i ich zbiorów.

5.7.2 Dane przenoszone winny być zabezpieczone przed dostępem osób trzecich, w szczególności:

a) fizyczne dokumenty winny być przenoszone w zalakowanych kopertach opisanych danymi kontaktowymi osoby przenoszącej dane,

b) dokumenty elektroniczne winny być zabezpieczone w sposób opisany w punkcie 5.3.5.b lub 5.3.5c, a 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. Odbiorca winien być poinformowany pisemnie o przesyłce, jej dacie oraz zawartości najpóźniej w dniu nadania przesyłki. Odbiorca obowiązany jest sprawdzić kompletność przesyłki w momencie jej odbioru.

5.8 Niszczenie danych

5.8.1 Dane osobowe i ich zbiory są przechowywane w IFMSA-Poland tak długo, jak ich przetwarzanie służy realizacji celów statutowych Stowarzyszenia, z uwzględnieniem zapisów Statutu i Regulaminu IFMSA-Poland.

5.8.2 Zgodnie z postanowieniem pkt IV pkt 4b załącznika do rozporządzenia kopie zapasowe winny być usunięte lub zniszczone niezwłocznie po ustaniu ich użyteczności.

5.8.3 Dane niszczone są wyłącznie, gdy są bezużyteczne i nie ma obowiązku ich przechowywania.

5.8.4 Osobą odpowiedzialną za zniszczenie danych lub ich zbiorów jest osoba administrująca tymi danymi lub ich zbiorem, po konsultacji ze swoim zwierzchnikiem lub Sekretarzem Generalnym IFMSA-Poland.

5.8.5 Zniszczenie danych fizycznych polega na zniszczeniu dokumentów uniemożliwiającym ich ponowne odczytanie, w szczególności z wykorzystaniem niszczarki.

5.8.6 Zniszczenie danych elektronicznych polega na trwałym usunięciu tych danych, a jeśli to możliwe także sformatowaniu nośnika.

5.8.7 Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

5.8.8 Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać, itp.).

5.8.9 Zniszczenie danych odnotowuje się poprzez sporządzenie protokołu zniszczenia, który należy przechowywać we właściwym archiwum IFMSA-Poland.

5.8.10 Wzór protokołu zniszczenia ustala Zarząd Główny 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 6
Postanowienia końcowe

6.1 We wszystkich kwestiach, których nie reguluje Polityka bezpieczeństwa IFMSA-Poland oraz instrukcja, o której mowa w punkcie 1.4, zastosowanie mają przepisy ustawy i przepisy rozporządzenia.

6.2 Wszelkie zmiany dotyczące Polityki bezpieczeństwa IFMSA-Poland podejmuje w drodze uchwały Zarząd Główny Stowarzyszenia.

6.3 Dokument wchodzi w życie z dniem uchwalenia.

6.4 Odpowiedzialność karna Administratora danych osobowych i osób administrujących danymi realizowana jest zgodnie z zapisami ustawy.

Załączniki do Polityki bezpieczeństwa IFMSA-Poland:

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w IFMSA-Poland.
2. Ewidencja osób wchodzących w skład podmiotu Administratora danych.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
4. Spis uchwał dotyczących wyglądu deklaracji i kwestionariuszy.
5. Upoważnienie do przetwarzania danych osobowych w IFMSA-Poland.

Podziękowania:

Dokument Polityki bezpieczeństwa IFMSA-Poland wraz z załącznikami powstał w okresie od marca do czerwca 2010 roku. Został zatwierdzony w czasie Zgromadzenia Delegatów w Legnicy dnia 26 marca 2010 roku, zaś przyjęty w głosowaniu Zarządu Głównego dnia 30 sierpnia 2010 roku. Za pomoc w przygotowaniu dokumentu dziękuję Joannie Ropie, Maciejowi Cyranowi oraz Członkom Zarządu Głównego kadencji 2010.

Aleksander Biesiada
Kraków, 6 września 2010 roku