POLITYKA BEZPIECZEŃSTWA

OCHRONY DANYCH OSOBOWYCH

CHRZEŚCIJAŃSKIEGO STOWARZYSZENIA DOBROCZYNNEGO

Rozdział 1

Postanowienia ogólne

§1

Polityka Bezpieczeństwa, zwana dalej ,,polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych pracowników i podopiecznych w Chrześcijańskim Stowarzyszeniu Dobroczynnym.

§2

Użyte w Polityce określenia oznaczają:

1)	Administrator Danych (ABI)	- Chrześcijańskie Stowarzyszenie Dobroczynne (ChSD), RR1 – Biuro Zarządu
2)	ustawa	- ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z pózn. zm.)
3)	rozporządzenie	- rozporządzanie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi 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 w ChSD .
5)	Administrator Bezpieczeństwa Informacji ChSD	- osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w ChSD
6)	Administrator Bezpieczeństwa Informacji (RR1, RW1, RW2, RW3, AK, GG)	- osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w: RR1 - Biuro Zarządu RW1 - Odziały i placówki ChSD RW2 - Biuro Obsługi Dotacji / zadania RW3 - Biuro Obsługi Projektu AK - Specjalista finansowy GG - Dział Księgowości Głównej

7)	Administrator Bezpieczeństwa Informacji (RO1, AK)	- osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu ChSD, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych RO1 – Specjalista d.s. kadr AK – Specjalista finansowy
8)	Administrator Bezpieczeństwa Systemu Informatycznego (ABSI)	- osoba wyznaczona przez Administratora Danych do opieki nad systemem informatycznym ChSD
9)	Naruszenie zabezpieczenia ChSD	- jakiekolwiek naruszenie bezpieczeństwa, niezawodności, lub poufności
10)	Dane osobowe	- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
11)	Przetwarzanie danych osobowych	- jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych
12)	Usuwanie danych osobowych	- zniszczenie danych osobowych lub taką ich modyfikacje, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
13)	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
14)	Zabezpieczenie danych	- środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacja, ujawnieniem lub pozyskaniem danych osobowych bądź utratą
15)	Instrukcja	- Zarządzania Systemem Informatycznym dla systemu ChSD
16)	Pracownik	- osobę zatrudnioną w ChSD na podstawie stosunku pracy lub innego stosunku prawnego

Rozdział 2

Zakres oraz zasady zabezpieczania danych osobowych

§ 3

Niniejszą politykę stosuje się do zbioru osobowych pracowników i podopiecznych znajdujących się w placówkach i oddziałach ChSD.

§ 4

1) Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełnią Administrator Danych oraz RR1
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 ChSD, sprawuje Administrator Bezpieczeństwa Informacji ChSD.

§5

Dane osobowe przedstawione w ChSD podlegają ochronie zgodnie z przepisami ustawy.

§6

Przetwarzanie danych osobowych w ChSD jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielania wsparcia pracowników i podopiecznych, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli, związanych ze Statutowym działaniem Stowarzyszenia.

§7

Przetwarzanie danych osobowych w ChSD 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.

§8

w przypadku zbierania jakichkolwiek danych osobowych na potrzeby ChSD bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji o :

1) pełnej nazwie zadania oraz jego realizacji;
2) celu zbierania danych osobowych;
3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;

4) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie, zatrudnieniu czy tez wsparciu.

§9

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 w ChSD, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§10

1) Przetwarzanie danych osobowych znajdujących się w ChSD 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, czy standardy jakości samego ChSD.
2) Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych w ChSD powinny zostać przed podpisaniem , w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Administratora Bezpieczeństwa Informacji ChSD.

§11

Każdej osobie, której dane osobowe są przetwarzane w Stowarzyszeniu 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 uzupełniania, 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 kogo zostały zebrane.

§12

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:

1. jakie dane osobowe dotyczące zapytującej osoby są przetwarzane
2. w jaki sposób zebrano te dane osobowe
3. w jakim celu i zakresie te dane osobowe są przetwarzane
4. od kiedy są przetwarzane te dane osobowe
5. w jakim zakresie oraz komu te dane osobowe zostały udostępnione

§13

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane przez Administratora są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne realizacji celu, w jakim zostały zebrane, jest on 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 3
Obowiązki Administratora Bezpieczeństwa Informacji

§14

Administrator Bezpieczeństwa Informacji ChSD poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych w ChSD.

§15

Do zadań Administratora Bezpieczeństwa Informacji RR1 należy w szczególności:

1. współdziałanie z Administratorem Bezpieczeństwa Informacji w ChSD w zakresie zapewniającym wypełnienie obowiązków wynikających z ustawy i rozporządzenia;
2. prowadzenie i aktualizacja rejestru o którym mowa w §20, który stanowi załącznik nr1 do Polityki;
3. prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który stanowi załącznik nr2 do Polityki;
4. 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 ChSD (RR1);
5. opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w ramach realizowanych projektów podmiotowi zewnętrznemu wobec ChSD;
6. inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych.

§16

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

§17

1. Obowiązki Administratora Bezpieczeństwa Informacji ChSD w ramach realizowanych projektów i umów o dofinansowanie wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Zarządu ChSD (RR1)
2. Nadzór nad wykonywaniem obowiązków Administratora Bezpieczeństwa Informacji ChSD pełni osoba upoważniona do podejmowania decyzji w imieniu RR1 ChSD.

§18.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, Administrator Bezpieczeństwa Informacji ChSD konsultuje się i współpracuje z Administratorem Bezpieczeństwa Informacji RR1, RW2, RW3, RO1, AK, GG w zależności od potrzeb oraz RR1.

Rozdział 4

Przetwarzanie danych osobowych

§19.

1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę
2. Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką.
3. Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji.

§20.

1. Każdy pracownik mający dostęp do danych osobowych jest wpisywanie do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji ChSD.

2. Rejestr, o którym mowa w ust. 1, zawiera:
    1) imię i nazwisko pracownika:
    2) zakres przydzielonego uprawnienia;
    3) datę przyznania uprawnień;
    4) podpis Administrator Bezpieczeństwa Informacji ChSD potwierdzający przyznanie uprawnień;
    5) datę odebrania uprawnień
    6) podpis Administrator Bezpieczeństwa Informacji ChSD potwierdzający odebranie uprawnień.

§21.

1. Dopuszczenie do przetwarzania danych osobowych znajdujących się w ChSD przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskania pozytywnej opinii Administratora Bezpieczeństwa Informacji ChSD oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku §19 i 20 stosuje się odpowiedniego.
2. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§22.

Wszyscy pracownicy oraz osoby, o których mowa w §21 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.

§23.

Użytkownicy są w szczególności zobowiązani do:

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

§24.

Środki techniczne i organizacyjne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 4 do Polityki.

Rozdział 5

Postępowanie w przypadku naruszenia ochrony danych osobowych

§25

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

1. stwierdzono naruszenie zabezpieczenia ChSD;
2. 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;
3. inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w ChSD.

§26

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych jest zobowiązany do niezwłocznego poinformowania o tym bezpośrednio przełożonego oraz Administratora Bezpieczeństwa Informacji ChSD.
2. Administrator Bezpieczeństwa Informacji ChSD, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:

    - poinformować pisemnie o zaistniałym zdarzeniu RR1 ChSD i stosować się do jego zaleceń;
    - 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 ChSD, 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 w ChSD ;
    - 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:

a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
b) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
c) 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 ChSD w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
- przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych w ChSD.
-

4. Czynności opisane w ust. 3 wykonuje Administrator Systemu ChSD.

§27.

1. Po przywróceniu normalnego stanu ChSD 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 w ChSD.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań, a w przypadku gdy użytkownik nie jest pracownikiem, konsekwencje wynikające z umowy, o której mowa w §21 ust.1

§28.

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

Rozdział 6

Kontrola nad przestrzeganiem ochrony danych osobowych

§29.

1. Bieżąca kontrola nad przetwarzanie danych osobowych w ChSD jest dokonywana przez Administratora Bezpieczeństwa Informacji ChSD.
2. W ramach kontroli, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji ChSD jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymień Polityki

§30

1. Administrator Bezpieczeństwa Informacji ChSD przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.
2. Przygotowując raport, o którym mowa w §28.

§31.

Kontrola o której mowa w §30, polega w szczególności sprawdzeniu:

1. którzy pracownicy mają dostęp do danych osobowych;
2. czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osoba;
3. czy pracownicy i inne osoby, mające do danych przetwarzanych w ChSD posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 7
Postanowienia końcowe

§32

Polityka jest dokumentem wewnętrznym Stowarzyszenia i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§33.

Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych.

§34.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia ChSD.

§35.

1. Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji ChSD.
2. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych Administrator Systemu Informatycznego, o ile został powołany.

§36.

Integralną część niniejszej Polityki stanowią następujące załączniki:

1. Załącznik nr 1 - Rejestr osób upoważnionych do przetwarzania danych osobowych w ChSd;
2. Załącznik nr 2 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar., w którym są przetwarzane dane osobowe w ChSD;
3. Załącznik nr 3 - Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
4. Załącznik nr 4 – Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w ChSD.
5. Załącznik nr 5 - Klauzula informacyjna o przetwarzaniu danych osobowych pracowników i członków ChSD oraz odbiorców usług statutowych stowarzyszenia
6. Załącznik nr 6 – Klauzula zgody na przetwarzanie danych osobowych
7. Załącznik nr 7 – Oświadczenie