WEWNĘTRZNA POLITYKA OCHRONY DANYCH OSOBOWYCH OBOWIĄZUJĄCYCH W STOWARZYSZENIU

DIAKONIA RUCHU ŚWIATŁO-ŻYCIE

Przedmiotowa Wewnętrzna polityka ochrony, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w parafii *nazwa i miejscowość*, w tym z Dekretem ogólnym Konferencji Episkopatu Polski w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim z dnia 13 marca 2018 roku oraz z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. Administrator danych osobowych – Stowarzyszenie Diakonia Ruchu Światło-Życie

2. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych,

4. Użytkownik – osoba upoważniona przez Administratora Danych do przetwarzania danych osobowych,

5. Zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów,

6. Przetwarzanie danych – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych,

7. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w przypadku przetwarzania danych osobowych w takim systemie,

8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie,

9. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Stowarzyszeniu Diakonia Ruchu Światło-Życie, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.

3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych, a osoby te mają obowiązek się zapoznać z jej zasadami oraz ich przestrzegać, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią oraz jej rzetelnego stosowania w praktyce powierzonych zadań.

4. Dla skutecznej realizacji Polityki Administrator danych zapewnia:

a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

b) kontrolę i nadzór nad przetwarzaniem danych osobowych,

c) monitorowanie zastosowanych środków ochrony.

5. Monitorowanie przez Administratora danych zastosowanych środków ochrony obejmuje: działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi oraz podejmowanie działań, które mają zapobiec utracie danych albo ich zniszczeniu, rozumianemu jako skutek niezależnych od Administratora zdarzeń natury losowej.

6. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u Administratora danych.

1. Dane osobowe przetwarzane przez Administratora danych gromadzone są w zbiorach danych.

2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób.

3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.

4. Administrator danych prowadzi rejestr czynności przetwarzania, który podlega bieżącej aktualizacji.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora danych Wewnętrzną Polityką Ochrony, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w Stowarzyszeniu Diakonia Ruchu Światło-Życie.

2. Wszystkie dane osobowe w Stowarzyszeniu Diakonia Ruchu Światło-Życie są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:

a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.

b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty.

c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.

e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane, zgodnie z Rejestrem czynności przetwarzania danych osobowych, obowiązującym u Administratora.

f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.

g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią właściwych przepisów prawa Kościoła jak i prawa państwowego.

h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:

a) naruszenie bezpieczeństwa metod przechowywania danych oraz naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach, zwłaszcza poprzez korzystanie z prywatnych adresów elektronicznych, prywatnych profili na portalach

społecznościowych oraz podejmowania aktywności w Internecie, która nie jest związana z powierzonymi obowiązkami zawodowymi, na stanowiskach, na których są przetwarzane dane osobowe.

b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;

c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;

d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;

e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;

f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;

g) naruszenie praw osób, których dane są przetwarzane.

5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych,

6. Do obowiązków Administratora danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora danych na podstawie innych umów cywilnoprawnych) należy zapewnienie:

a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,

b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór Upoważnienia stanowi Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa

c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w placówce w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych".

7. Osoby upoważnione do przetwarzania danych osobowych oraz inne osoby, które mają dostęp do danych osobowych, choćby w ograniczonym zakresie zobowiązani są do:

a) ścisłego przestrzegania zakresu nadanego upoważnienia;

b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;

c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe Stowarzyszenia Diakonia Ruchu Światło-Życie, obejmuje trzy pomieszczenia Sekretariatu zlokalizowane w Centrum Ruchu Światło-Życie w Krościenku n. Dunajcem ul. Ks. F. Blachnickiego 2.

2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, a środki te obejmują:

a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.

b) zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.

c) wykorzystanie zamykanych szaf i sejfów do zabezpieczenia dokumentów.

d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.

e) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.

f) ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem poprzez instalację specjalistycznego oprogramowania ochronnego

g) Zabezpieczenie dostępu do urządzeń na których są przetwarzane dane przy pomocy haseł dostępu.

i) Wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.

2. Przed powierzeniem przetwarzania danych osobowych Administrator winien uzyskać na piśmie informacje o zasadach ochrony przetwarzania danych osobowych, które istnieją w podmiocie, któremu przekazano dane osobowe.

VIII. Postanowienia końcowe,

1. Za niedopełnienie, choćby nieumyślne obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych.

2. Integralną część niniejszej Polityki bezpieczeństwa stanowi załącznik nr 1 Wzór upoważnienia do przetwarzania danych osobowych.