Polityka Bezpieczeństwa
Przetwarzania danych osobowych

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W CARITAS ARCHIDIECEZJI GDAŃSKIEJ

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:

Podpis Inspektora Ochrony Danych:	Data:	Podpis Administratora Systemu Informatycznego:	Data:

Spis treści

Wstęp

Realizując postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) oraz wydane w oparciu o delegacje ustawą przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004r. (Dz.U. z 2004 r. nr 100, poz. 1024 z zm.) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

Jako załącznik do niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.
Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych.
2. Administrator Danych Osobowych – Caritas Archidiecezji Gdańskiej z siedzibą przy Al. Niepodległości 778, 81 - 805 Sopot, decydująca o celach i środkach przetwarzania danych osobowych.

3. Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za organizację ochrony danych osobowych. IOD posiada odpowiednią wiedzę w zakresie ochrony danych osobowych (załącznik nr 4a do Polityki Bezpieczeństwa).
4. RODO – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych).
5. Rozporządzenie – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 1998 r. nr 80, poz. 521 z zm.).
6. Dane osobowe (dane) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
7. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów.
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
9. Zgoda osoby, której dane dotyczą – rozumie się przez to dobrowolne oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych we wskazanym celu tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
10. Zbiór danych osobowych – zbiór uporządkowanych, powiązanych ze sobą tematycznie zapisanych danych. Zbiór danych jest złożony z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisane dane osobowe.
11. Przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
13. Administrator systemu informatycznego – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.

14. Użytkownik – pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków.
15. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
16. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. płytki CD/DVD/BR, pendrive'y, dyski twarde, karty flash etc.

Rozdział 1. Inspektor Ochrony Danych

§1

Do najważniejszych obowiązków Inspektora Ochrony Danych należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki,
3. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych dla osób przetwarzających te dane (Załącznik nr 3),
4. prowadzenie ,,Rejestru czynności przetwarzania danych osobowych" (Załącznik nr 5),
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

§2

Inspektor Ochrony Danych ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,
2. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,

3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Rozdział 2. Zasady przetwarzania i ochrony danych osobowych

§ 1

1. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem.
2. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy mają obowiązek:
   1) zapoznać się (i podpisać stosowne oświadczenie potwierdzające ww. czynność) z obowiązującymi zasadami ochrony danych osobowych określonymi w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi
   2) podpisać oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczenia (np. hasła dostępowe) w tajemnicy (załącznik nr 4 do Polityki Bezpieczeństwa)
3. Organizacja przetwarzania danych osobowych w Organizacji opiera się na wyodrębnieniu następujących kategorii osób:
   1) ADO;
   2) IOD;
   3) ASI;
   4) Użytkowników (osoby upoważnione do przetwarzania danych osobowych przez ADO lub przez podmioty zewnętrzne);
   5) Personel pomocniczy (np. osoby sprzątające biuro, itp.) wyłącznie w obecności przebywającego w obszarze przetwarzania danych osobowych bez ich przetwarzania zgodnie z nadanym upoważnieniem (załącznik nr 6 do Polityki Bezpieczeństwa) oraz po odnotowaniu tego faktu w ewidencji prowadzonej dla ww. osób.

§ 2

Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania") stanowi załącznik nr 1 do niniejszego dokumentu.

§ 3

Wymagany przez rozporządzenie wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 2 do niniejszego dokumentu.

§ 4

1. Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 3 do niniejszego dokumentu) oraz podpisać oświadczenie o zachowaniu poufności tych danych (załącznik nr 4 do niniejszego dokumentu).
2. Każda osoba mająca dostęp do danych została zapoznana z zasadami bezpiecznego przetwarzania danych wynikającymi z niniejszej Polityki oraz Instrukcji Zarządzania.
3. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe posiadają tylko osoby upoważnione.
4. Dostęp do komputerów, na których są przetwarzane dane osobowe posiadają tylko osoby upoważnione.
5. Osoby mające dostęp do danych osobowych zobowiązane są, na mocy niniejszej Polityki, do zachowania danych osobowych oraz informacji o sposobach ich zabezpieczenia w tajemnicy.
6. W Organizacji prowadzony jest, nakazany przez RODO rejestr czynności przetwarzania danych osobowych (załącznik nr 5 do niniejszego dokumentu).
7. Prowadzona jest dokumentacja obejmująca Politykę Bezpieczeństwa oraz Instrukcję Zarządzania.

§ 5

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części II § 2 Instrukcji Zarządzania Systemem Informatycznym.

§ 6

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu

poufności (załącznik nr 4 do niniejszego dokumentu), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

§ 7

1. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 28 RODO. Zalecany wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 6 do Polityki Bezpieczeństwa.

2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego administratora danych osobowych.

3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.

4. Wykaz podmiotów, którym instytucja na podstawie istniejących umów powierza dane osobowe stanowi załącznik nr 7 do Polityki.

§ 8

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności właściwie umotywowany wniosek podmiotu uprawnionego.

§ 9

1. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

2. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

3. W firmie stosowane są następujące zabezpieczenia:

   1) biuro zabezpieczone jest zamykanymi drzwiami,
   2) biuro zabezpieczone jest systemem alarmowym,
   3) biuro poza godzinami pracy chronione jest przez służbę ochrony,
   4) komputery służące do przetwarzania danych osobowych chronione są przez program antywirusowy,
   5) dostęp do komputerów zabezpieczony jest poprzez uwierzytelnienie (login i min. 8 znakowe hasło, skomplikowane – składające się z małych, wielkich liter, znaków specjalnych lub cyfr),

6) hasła zmieniane są co 30 dni,
7) dostęp do aplikacji służących do przetwarzania danych osobowych zabezpieczony jest poprzez uwierzytelnienie (login i min. 8 znakowe hasło, skomplikowane – składające się z małych, wielkich liter, znaków specjalnych lub cyfr),
8) dostęp do serwera posiadają wyłącznie upoważnieni pracownicy,
9) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
10) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,
11) biuro wyposażone jest w niszczarki,
12) biuro wyposażone jest w wolnostojącą gaśnicę.

§ 10

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Organizacji”

§ 11

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, osoba wyznaczona przez osobę nadzorującą przetwarzanie danych przygotowuje odpowiedź w ciągu 30 dni.

§ 12

W przypadku zbierania danych osobowych od osoby, której one dotyczą, jest ona informowana w przystępnej dla niej formie o:

1) adresie siedziby i pełnej nazwie,

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

3) prawie dostępu do treści swoich danych oraz ich poprawiania,

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,

5) prawie do bycia zapomnianym.

Wzór oświadczenia informacyjnego dla osoby, której dane osobowe są zbierane w ramach działań podejmowanych przez Caritas Archidiecezji Gdańskiej stanowi załącznik nr 4b do Polityki

Rozdział 3. Instrukcja alarmowa

§1

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

§2

Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych zobowiązany jest poinformować bezpośredniego przełożonego lub Inspektora Ochrony Danych.

§3

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

§4

Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

§5

W przypadku stwierdzenia wystąpienia zagrożenia Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
2) inicjuje ewentualne działania dyscyplinarne,
3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
4) dokumentuje prowadzone postępowania.

§6

W przypadku stwierdzenia incydentu (naruszenia) Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
2) zabezpiecza ewentualne dowody,
3) ustala osoby odpowiedzialne za naruszenie,
4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
5) inicjuje działania dyscyplinarne,
6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
7) dokumentuje prowadzone postępowania.

Dodatkowo, Inspektor Ochrony Danych, bez zbędnej zwłoki, jednak nie później niż w terminie 72 godzin (kalendarzowych) po stwierdzeniu naruszenia zgłasza je właściwemu organowi nadzorczemu- Urzędowi Ochrony Danych Osobowych oraz osobie, której dane uległy naruszeniu.

Rozdział 4. Procedura działań korygujących i zapobiegawczych

§1

Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.

§2

Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

§3

Osobą odpowiedzialną za nadzór nad procedurą jest Inspektor Ochrony Danych.

Rozdział 5. Postanowienia końcowe

§1

Corocznie do dnia 30 października, IOD lub wyznaczony przez Administratora danych pracownik przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych, w oparciu o przeprowadzony plan audytów (załącznik nr 9)
W spotkaniu sprawozdawczym uczestniczą: Przedstawiciel Administratora danych oraz IOD. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział: inni członkowie jednostki, informatyk, kierownicy działów/jednostek.
Sprawozdanie przygotowywane jest w formie pisemnej.

§2

Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Polityki bezpieczeństwa każdego użytkownika.

§3

Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

§4

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

§5

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

§6

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z

określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

§7

Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z RODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§8

W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy RODO oraz wydane na jego podstawie akty wykonawcze.

§9

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 roku.

§ 10

Aktualizacji niniejszej Polityki dokonuje Inspektor Ochrony Danych przy współpracy z Administratorem Systemu Informatycznego.

……..……
podpis w imieniu Organizacji

Załączniki:

1. Wykaz pomieszczeń w których przetwarzane są dane osobowe (Załącznik 1).
2. Wykaz zbiorów danych osobowych (Załącznik 2).
3. Upoważnienie do przetwarzania danych osobowych (Załącznik 3).
4. Oświadczenie (Załącznik 4).
5. Upoważnienie dla Inspektora Ochrony Danych (IOD) (Załącznik 4a)
6. Oświadczenie osoby, której dane podlegają przetwarzaniu (Załącznik 4b)
7. Rejestr czynności przetwarzania danych osobowych (Załącznik 5).
8. Umowa powierzenia przetwarzania danych osobowych (Załącznik 6).
9. Rejestr podmiotów zewnętrznych, którym zostało powierzone przetwarzanie danych osobowych (Załącznik 7).

10. Rejestr udostępnionych danych osobowych organom uprawnionym i podmiotom trzecim (Załącznik 8).
11. Plan audytów (Załącznik 9).