Polityka ochrony danych osobowych
przetwarzanych w związku z celami statutowymi
wraz z oceną ich ryzyka
w Parafii Ewangelicko-Augsburskiej w Ostródzie

zatwierdzona po raz pierwszy w dniu 10 lipca 2024 r.

Wprowadzenie

Polityka ochrony danych osobowych przetwarzanych w związku z celami statutowymi określa zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Regulaminu Ochrony Danych Osobowych Kościoła Ewangelicko-Augsburskiego w Rzeczypospolitej Polskiej z dnia 23 kwietnia 2018 r., przyjętego Uchwałą Rady Synodalnej Kościoła nr RS/XIV/12/1/2018 (dalej określanego jako „Regulamin" lub „RODOK"), w związku z 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.

I. Definicje

W niniejszej Polityce:

1. **„dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji lub identyfikator internetowy;
2. **„przetwarzanie"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3. **„zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4. **„administrator"** oznacza jednostkę organizacyjną Kościoła, w tym Parafię, Diecezję, Diakonat i inną kościelną osobę prawną, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
5. **„podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, bądź jednostkę organizacyjną, która przetwarza dane osobowe w imieniu administratora;
6. **„zgoda"** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie

oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

7. **„naruszenie ochrony danych osobowych”** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
8. **„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
9. **„szczególne kategorie danych osobowych”** oznacza dane osobowe, o których mowa w art. 9 ust. 1 Rozporządzenia, w tym dotyczące przekonań religijnych;
10. „**struktura Kościoła”** oznacza Kościół jako całość, wszystkie jego osoby prawne i inne jednostki organizacyjne nieposiadające osobowości prawnej;
11. **„organ nadzorczy” lub „komisja” lub „KODO”** oznacza Komisję Ochrony Danych Osobowych Kościoła Ewangelicko-Augsburskiego w Rzeczypospolitej Polskiej, bądź Ewangelicką Komisję Wspólną Ochrony Danych Osobowych, jeśli zostanie taka powołana.

II. Przetwarzanie danych i ich zbiory

Administrator przetwarza dane osobowe w związku z pełnionymi funkcjami statutowymi, korzystając przy tym z autonomii oraz niezależności gwarantowanej w szczególności przez art. 25 ust. 5 i art. 53 ust. 7 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. oraz Ustawę z dnia 13 maja 1994 r. o stosunku Państwa do Kościoła Ewangelicko-Augsburskiego w Rzeczypospolitej Polskiej (Dz.U. z 1994 r. Nr 73, poz. 323 z późn. zm.). Przetwarzanie danych osobowych przez administratora, w tym szczególnych kategorii danych osobowych określonych w obowiązujących przepisach prawa, w szczególności dotyczących przekonań religijnych, jest niezbędne do realizacji przez administratora i Kościół funkcji statutowych.

Tam, gdzie jest to konieczne dla wykonywania obowiązków wynikających z przepisów prawa kościelnego lub przepisów prawa powszechnie obowiązującego lub dyspozycji osoby, której dane dotyczą, Kościół przekazuje dane w ramach struktur Kościoła, w szczególności do innych Parafii, Diecezji, Konsystorza lub duszpasterzy środowiskowych z zachowaniem przepisów Regulaminu, bądź do organów publicznych w związku z obowiązkiem prawnym.

Nazwa zbioru	Główny zbiór parafialny
Cel przetwarzania	Cele statutowe Kościoła w zakresie działalności parafialnej
Charakter i zakres danych osobowych	Dane dotyczące tożsamości, adresu zamieszkania/zameldowania, korespondencyjnego danych; otrzymanych Sakramentów, korzystania z czynności kościelnych, zaangażowania kościelnego, korzystania ze spotkań kościelnych, przynależności religijnej i konfesyjnej obecnych i przeszłych, pełnionych funkcjach religijnych – kontaktowych członków Kościoła, byłych członków Kościoła i

	osób utrzymujących stałe kontakty z Kościołem w związku z jego celami statutowymi.
Opis operacji przetwarzania	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie w ramach następujących podzbiorów: - kartoteka parafialna; - księgi metrykalne takie jak Księga Urodzeń i Chrztów, Księga Ślubów, Księga Zgonów i Pogrzebów; - dokumenty parafialne takie, jak Kartoteka Parafialna, Księga Konfirmantów, Księga Wstąpień i Wystąpień, Księga Zapowiedzi Małżeńskich, Księga Odwiedzin i Komunii Domowych, księgi pomocnicze dla zgłaszanych Chrztów, ślubów, pogrzebów, modlitw przyczynnych i wspomnień, Kronika Parafialna, protokoły wstąpień do Kościoła i wystąpień, zbiory odpisów metryk Chrztów, poświadczeń albo kopii wydanych odpisów metryk Chrztów z zaznaczeniem celu wydania, kart zgonów, dyspens na ślub wyznaniowo mieszany i osób rozwiedzionych, zaświadczeń Urzędu Stanu Cywilnego stwierdzających brak przeszkód zawarcia małżeństwa; - dokumentacji cmentarnej, w części zawierającej dane osób żyjących; - inne związane z przetwarzaniem danych dotyczących Sakramentów i czynności kościelnych, nauczania religii oraz funkcjonowania Parafii w zakresie celów statutowych. Zbiór prowadzony elektronicznie i papierowo.
Uwagi	Okres przetwarzania zgodnie z przepisami prawa kościelnego; zbiór szczególnie chroniony w związku z przechowywaniem danych o charakterze sakralnym

Nazwa zbioru	Zbiór danych wyborczych i funkcji kościelnych
Cel przetwarzania	Cele statutowe Kościoła w zakresie powoływania władz kościelnych, innych funkcji i przygotowywania do urzędu duchownego.
Charakter i zakres danych osobowych	Dane niezbędne do prowadzenia rejestrów wyborczych, protokołów wyborczych, list wyborczych, jak również dane kandydatów, dane osób sprawujących obecnie lub w przeszłości funkcje kościelne, duchownych, osób przygotowujących się do okresu kandydackiego lub w okresie kandydackim do urzędu duchownego – w zakresie wymaganym przez przepisy kościelne lub w celu wykonania obowiązku, umowy bądź oczekiwania osoby, której dane dotyczą.
Opis operacji przetwarzania	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub

	niszczenie. Zbiór prowadzony elektronicznie i papierowo.
Uwagi	Okres przetwarzania zgodnie z przepisami prawa kościelnego; zbiór szczególnie chroniony w związku z przechowywaniem danych o charakterze sakralnym

Nazwa zbioru	Parafialne dane finansowe
Cel przetwarzania	Cele statutowe Kościoła w zakresie prowadzenie księgowości parafialnej oraz innych wymaganych prawem rejestrów o charakterze finansowym na rzecz kultu religijnego lub innej działalności związane z celami statutowymi, w tym dotyczących umów cywilnoprawnych.
Charakter i zakres danych osobowych	Dane osobowe powiązane z informacjami dotyczącymi przychodów i rozchodów parafii, w tym darczyńców, osób wnoszących składki kościelne, stron umów cywilnoprawnych, korzystające z pomocy materialnej Parafii oraz wnoszących opłaty związane z cmentarzem.
Opis operacji przetwarzania	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Zbiór prowadzony elektronicznie i papierowo.
Uwagi	Okres przetwarzania zgodnie z przepisami prawa kościelnego i powszechnie obowiązującego; zbiór szczególnie chroniony w związku z przechowywaniem także danych o charakterze sakralnym.

Nazwa zbioru	Dane osobowe związane z działalnością wydawniczą statutową
Cel przetwarzania	Cele statutowe Kościoła w zakresie wydawnictw kościelnych (książki, czasopisma) i kolportażu wydawnictw kościelnych
Charakter i zakres danych osobowych	Dane niezbędne do prowadzenia działalności statutowej w zakresie wydawnictw kościelnych (książki, czasopisma, druki ulotne) i kolportażu wydawnictw kościelnych, m.in. dotyczące tożsamości, adresu korespondencyjnego, danych kontaktowych, nabywanych wydawnictw, jak również dane autorów, współpracowników, wydawców i innych osób uczestniczących w procesie wydawniczym.
Opis operacji przetwarzania	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Zbiór prowadzony elektronicznie i papierowo.
Uwagi	Okres przetwarzania zgodnie z przepisami prawa kościelnego i

	powszechnie obowiązującego.

III. Ocena legalności przetwarzania danych osobowych

Administrator określił, że wszystkie dane osobowe przetwarzane są zgodnie z § 3 RODOK, tj. dane osobowe są:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2) zbierane w konkretnych, wyraźnie określonych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4) prawidłowe i w razie potrzeby uaktualniane („prawidłowość”);
5) przechowywane zgodnie z wymogami prawa kościelnego i przepisów powszechnie obowiązujących („ograniczenie przechowywania”);
6) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; przy czym dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych („ograniczenie przechowywania”);
7) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
8) przetwarzane w sposób umożliwiający administratorowi wykazanie, że prawo dotyczące ochrony danych osobowych jest przestrzegane („rozliczalność”).

Jednocześnie stwierdzono brak potrzeby powierzenia przetwarzania danych osobowych innym podmiotom.

IV. Rejestr czynności przetwarzania danych osobowych

Administrator prowadzi w formie dokumentowej, w tym w formie elektronicznej, rejestr czynności przetwarzania danych osobowych, który obejmuje:

a) nazwę administratora oraz jego dane kontaktowe, jak również inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
e) gdy ma to zastosowanie, informacje dotyczące przekazania danych osobowych poza terytorium Rzeczypospolitej Polskiej;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Administrator ma obowiązek udostępnienia rejestru na żądanie organu nadzorczego.
Wzór rejestru określony jest Załącznikiem do niniejszej Polityki.

V. Ocena ryzyka

Zgodnie z § 19 RODOK, w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z prawem, administrator powinien oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki minimalizujące to ryzyko. W tym celu administrator dokonał oceny ryzyka w zakresie bezpieczeństwa danych, biorąc pod uwagę:

- przypadkowe lub niezgodne z prawem zniszczenie, utracenie lub zmodyfikowanie danych osobowych;
- nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Analiza przeprowadzona jest w oparciu o dwa wymiary: prawdopodobieństwo wystąpienia zdarzenia oraz stopień skutków prawdopodobnego naruszenia, której dane są przetwarzane. Poziom ryzyka przetwarzania danych określa się dla poszczególnych zbiorów danych zgodnie z poniższą tabelą przyjmując jako wynik oceny ryzyka ocenę określoną dla przecięcia się linii poziomej i pionowej zgodnie z opisem danego kwadratu (analiza graficzna). Przy czym:

- jeśli inne czynniki niż wysokie ryzyko naruszenia lub poziom wyrządzonej szkody, powodują potrzebę podwyższenia ryzyka, należy przyjąć wyższy poziom ryzyka;
- świadome naruszenie prawa przez administratora jest zawsze określane jako ryzyko wysokie i nie może być podejmowane.

ANALIZA GRAFICZNA RYZYKA

Wysokie ryzyko naruszenia (częściej niż raz na rok)	**Ryzyko średnie *(Pole 41)***	**Ryzyko wysokie *(Pole 42)***	**Ryzyko wysokie *(Pole 43)***	**Ryzyko wysokie *(pole 44)***
Średnie ryzyko naruszania (rzadziej niż raz na rok)	**Ryzyko średnie *(Pole 31)***	**Ryzyko średnie *(Pole 32)***	**Ryzyko wysokie *(Pole 33)***	**Ryzyko wysokie *(Pole 34)***
Umiarkowane ryzyko naruszenia (rzadziej niż raz na 3 lata)	**Ryzyko niskie *(Pole 21)***	**Ryzyko średnie *(Pole 22)***	**Ryzyko średnie *(Pole 23)***	**Ryzyko wysokie (*Pole 24)***
Niskie ryzyko naruszenia (rzadziej niż raz na 5 lat)	**Ryzyko niskie *(Pole 11)***	**Ryzyko niskie *(Pole 12)***	**Ryzyko średnie *(Pole 13)***	**Ryzyko średnie *(Pole 14)***
	Niski poziom	Umiarkowany	Średni poziom	Wystąpienie

	szacowanych szkód majątkowych lub niemajątkowych (wartość >10 tyś. PLN)	poziom szacowanych szkód majątkowych lub niemajątkowych (wartość >50 tyś. PLN)	szacowanych szkód majątkowych lub niemajątkowych (wartość >100 tyś. PLN)	uszczerbku fizycznego lub wysoki poziom szacowanych szkód majątkowych lub niemajątkowych (wartość >200 tyś. PLN)

WYNIK OCENY RYZYKA DLA POSZCZEGÓLNYCH ZBIORÓW LUB OPERACJI PRZETWARZANIA

Nazwa zbioru	Wynik oceny ryzyka
Główny zbiór parafialny	Poziom średni (pole 22)
Zbiór danych wyborczych i funkcji kościelnych	Poziom niski (pole 11)
Parafialne dane finansowe	Poziom średni (pole 23)
Dane osobowe związane z działalnością wydawniczą statutową	Poziom niski (pole 21)

W wyniku analizy określono, że nie występują operacje przetwarzania danych, które mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

VI. Upoważnienia

Administrator odpowiada za nadawanie, zmianę i odbieranie upoważnień do przetwarzania danych w zbiorach manualnych (papierowych) i systemach informatycznych. W tym celu prowadzi się Ewidencję upoważnionych osób do przetwarzania danych, stanowiącą Załącznik do niniejszej Polityki. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa w zakresie wskazanym w ewidencji.

VII. Postępowanie z incydentami naruszenia ochrony danych

Zgodnie z § 20 RODOK:

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu oraz swojej władzy przełożonej, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu lub swojej władzy przełożonej po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa w pkt 1, musi co najmniej:
    1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i szacunkową liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2) zawierać imię i nazwisko oraz dane kontaktowe inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator, bez zbędnej zwłoki, zawiadamia jasnym i prostym językiem osobę, której dane dotyczą, o takim naruszeniu.
6. Z obowiązku, określonego w pkt 4, administrator jest zwolniony, jeśli:
    a) wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; lub
    b) zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
    c) wymagałoby to nadmiernego wysiłku, wówczas zobowiązany jest do wydania publicznego komunikatu lub zastosowanie podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

VIII. Inne postanowienia

Zbiory danych osobowych przechowywane papierowo, sprzęt komputerowy oraz nośniki danych zawierające dane osobowe powinny być przechowywane w pomieszczeniach zamkniętych wyposażonych w wystarczającą ochronę przed kradzieżą i włamaniem, a w przypadku gdy do danego pomieszczenia ma dostęp choćby jedna osoba nieupoważniona do przetwarzania danych – dodatkowo w szafach zamykanych. Klucze do takiego pomieszczenia powinny być przechowywane z odpowiednią starannością, a przebywanie osób trzecich, jeśli jest konieczne, powinno następować pod stałą kontrolą osoby upoważnionej do przetwarzania danych lub osoby odpowiedzialnej za nią.

Każda osoba przed dopuszczeniem do czynności przetwarzania danymi osobowymi powinna być przeszkolona przez osobę odpowiedzialną za przetwarzanie danych osobowych lub osobę przez nią wyznaczoną. Należy sporządzić notatkę z przeszkolenia poprzez określenia imion i

nazwisk szkolonego i szkolącego oraz datę i miejsce szkolenia, jak również potwierdzenie tego faktu odbycia szkolenia przez podpisami szkolonego i szkolącego.

Należy co roku dokonywać weryfikacji potrzeby ponownej oceny ryzyka i aktualizować dokumenty o wyniki takiej analizy.

Potwierdzam zatwierdzenie do stałego użytku przez Radę Parafialną

Metryka aktualizacji dokumentu

Data aktualizacji dokumentu	Organ władzy kościelnej zatwierdzający aktualizację