Regulamin ochrony danych osobowych
Polskiego Autokefalicznego Kościoła Prawosławnego

Rozdział I

Zasady ogólne

§ 1

1. Polski Autokefaliczny Kościół Prawosławny, zwany w dalszej części Regulaminu Kościołem, 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 roku oraz Ustawę z dnia 4 lipca 1994 roku o stosunku Państwa do Polskiego Autokefalicznego Kościoła Prawosławnego (Dz.U. z 2014 r. poz. 1726) oraz ustawę o gwarancjach wolności sumienia i wyznania z dnia 17 maja 1989 roku (Dz.U. z 2017 r. poz. 1153).
2. Przetwarzanie danych osobowych przez kościelnych administratorów danych osobowych (osoby prawne Kościoła lub jego inne jednostki organizacyjne), w tym szczególnych kategorii danych osobowych, o których mowa w Rozporządzeniu, w szczególności dotyczących przekonań religijnych, jest niezbędne do realizacji przez Kościół jego funkcji statutowych.
3. Niniejszy Regulamin stosuje się do wszelkich operacji przetwarzania danych osobowych przez wszystkie jednostki organizacyjne Kościoła, w tym osoby prawne Kościoła, z wyjątkiem operacji przetwarzania związanych z prowadzeniem przez nie działalności gospodarczej lub innej, wykraczającej poza funkcje statutowe.
4. Na użytek niniejszego Regulaminu:
   a) „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowanią osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczną 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;
   b) „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
   c) „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, w szczególności zbiorami danych są: księgi metrykalne (księgi chrztów, ślubów, pogrzebów), księgi parafialne, zbiory danych osób, którym udzielane jest wsparcie lub pomoc w ramach działalności charytatywno – opiekuńczej przez Kościelne jednostki organizacyjne, zbiory danych osób pełniących posługę duszpasterską, zbiory danych pracowników, współpracowników zatrudnionych przez Kościelne osoby prawne;
   d) „administrator" oznacza osobę prawną lub inną jednostkę organizacyjną, która ustala cele i sposoby przetwarzania danych osobowych.

e) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, bądź jednostkę organizacyjną, która przetwarza dane osobowe w imieniu administratora;

f) „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;

g) „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;

h) „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;

i) „Rozporządzenie” oznacza 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);

j) „prawo o ochronie danych osobowych” oznacza przepisy niniejszego Regulaminu oraz przepisy powszechnie obowiązujące niesprzeczne z objętymi konstytucyjnymi autonomią i niezależnością prawem wewnętrznym Kościoła oraz jego doktryną;

k) „szczególne kategorie danych osobowych” oznacza dane osobowe, o których mowa w art. 9 ust. 1 Rozporządzenia, w tym dotyczące przekonań religijnych;

l) „struktura Kościoła” oznacza Kościół jako całość, wszystkie jego osoby prawne i inne jednostki organizacyjne nieposiadające osobowości prawnej;

m) „organ nadzorczy” lub „KIODO PAKP” oznacza Kościelnego Inspektora Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego;

n) „Kościół” lub „PAKP” oznacza Polski Autokefaliczny Kościół Prawosławny.

§ 2

1. Przetwarzając dane osobowe Kościół jako całość oraz jego jednostki organizacyjne są zobowiązane do przestrzegania powszechnie obowiązujących przepisów prawa dotyczących przetwarzania danych osobowych, w tym w szczególności przepisów Rozporządzenia oraz niniejszego Regulaminu.
2. Niezbędne do realizacji celów Kościoła jest przetwarzanie szczególnych kategorii danych osobowych, dokonywane w ramach uprawnionej działalności, z zachowaniem odpowiednich zabezpieczeń, dotyczące obecnych oraz byłych członków Kościoła oraz osób utrzymujących stałe kontakty z Kościołem w związku z jego celami statutowymi.
3. Szczególne kategorie danych osobowych osób nie będących członkami Kościoła, nie będących byłymi członkami Kościoła lub nie będących osobami utrzymującymi stałe kontakty z Kościołem nie mogą być przetwarzane bez pisemnej wyraźnej zgody tych osób na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach.

Rozdział II

Przetwarzanie danych

§ 3

Dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada legalności, rzetelności i przejrzystości przetwarzania);

2) zbierane w konkretnych, wyraźnie określonych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych, do badań naukowych lub historycznych albo do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami (zasada ograniczenia celu);

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);

4) prawidłowe i w razie potrzeby uaktualniane (zasada prawidłowości);

5) przechowywane zgodnie z wymogami prawa kościelnego i przepisów powszechnie obowiązujących;

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; 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, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (zasada ograniczenia przechowywania - czasowości);

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 (zasada integralności i poufności);

8) przetwarzane w sposób umożliwiający określenie, czy prawo dotyczące ochrony danych osobowych jest przestrzegane (zasada rozliczalności).

§ 4

1. Przetwarzanie danych osobowych jest możliwe tylko w stosunku do danej osoby wyłącznie wtedy, gdy spełniony jest co najmniej jeden z poniższych warunków:

   a) osoba, której dane dotyczą została ochrzczona w Kościele lub wstąpiła do Kościoła zgodnie z przepisami prawa kościelnego;

   b) osoba, której dane dotyczą nie posiadała zdolności do czynności prawnych, a została włączona do Kościoła na podstawie wyrażonej woli przynajmniej jednego z rodziców lub opiekunów prawnych;

   c) osoba, której dane dotyczą utrzymuje stałe kontakty z Kościołem w związku z jego celami statutowymi;

d) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów, bądź też uczynił to przynajmniej jeden z jej rodziców lub opiekun prawny;

e) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

f) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

g) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

h) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

i) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Wystąpienie z Kościoła zgodnie z przepisami prawa kościelnego nie pozbawia Kościół prawa do przetwarzania danych takiej osoby, gdy jest to niezbędne do wykonywania celów statutowych, w szczególności poprzez przechowywanie danych w kartotekach parafialnych i księgach metrykalnych.

3. Przetwarzanie danych wrażliwych możliwe jest wyłącznie w stosunku do obecnych oraz byłych członków Kościoła oraz osób utrzymujących kontakty z Kościołem w związku z jego celami statutowymi w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń.

§ 5

1. Zabrania się ujawniania danych osobowych poza struktury Kościoła, bez zgody osoby, której dane dotyczą, w szczególności poprzez ich zamieszczanie w dostępnych miejscach publicznych.

2. Ujawnianie lub przekazywanie danych osobowych osób, których dane dotyczą, w ramach struktur Kościoła, w tym ujawniania danych podczas nabożeństw zgodnie z przyjętą praktyką w Kościele, wymaga zgody osoby, której dane miałyby zostać ujawnione lub przekazane.

3. Zakazu ujawniania danych osobowych nie stosuje się, jeżeli ujawnienie danych jest związane z pełnieniem funkcji duchownego lub ubieganiem się o niego, pełnieniem urzędu lub funkcji w Kościele lub jednostkach organizacyjnych Kościoła (z wyboru lub mianowania) – w zakresie bezpośrednio związanym z pełnieniem danego urzędu lub funkcji lub wynikającym z utrwalonego zwyczaju kościelnego, o ile nie narusza to godności takiej osoby.

4. Kalendarze, roczniki, informatory i inne publikacje mogą zawierać dane publicznych kościelnych osób prawnych i osób upoważnionych do ich reprezentowania.

Rozdział III

Prawa osoby, której dane są przetwarzane

§ 6

1. Jeżeli dane osobowe zbierane są od osoby, której te dane dotyczą, administrator zobowiązany jest do powiadomienia jej o przetwarzaniu, uwzględniając przy tym co najmniej poniższe informacje:
   a) nazwę administratora i dane kontaktowe;
   b) dane kontaktowe inspektora ochrony danych dla danego administratora jeżeli został powołany;
   c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   d) możliwość przekazywania danych do innych administratorów w ramach struktur Kościoła lub innych administratorów, jeśli jest to planowane;
   e) okres, przez który dane osobowe będą przechowywane, z zastrzeżeniem, że przetwarzania danych osobowych dla celów statutowych Kościoła, oznacza co do zasady ich bezterminowe przechowywanie zgodnie z obowiązującymi przepisami dotyczącymi archiwizacji zasobów metrykalnych;
   f) prawo do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, przy czym danych przetwarzanych w związku z wypełnianymi funkcjami statutowymi Kościoła nie można usunąć;
   g) prawo wniesienia skargi do organu nadzorczego;
   h) podanie danych osobowych jest wymogiem ustawowym lub wynika z prawa kościelnego lub jego doktryny religijnej lub stanowi warunek zawarcia umowy bądź czynności kościelnej oraz osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   i) dodatkowo w przypadku, gdy do przetwarzania wymagana była zgoda danej osoby, informacje o prawie do cofnięcia zgody w dowolnym momencie.
2. Jeżeli dane zostały pozyskane inaczej niż od danej osoby, należy dodatkowo taką osobę poinformować o kategorii przetwarzanych danych osobowych oraz źródle uzyskania danych osobowych w terminie nie dłuższym niż jeden miesiąc.
3. Obowiązek udzielenia informacji nie ma zastosowania, jeżeli:
   a) osoba, której dane dotyczą, dysponuje już tymi informacjami, lub
   b) utrwalenie lub ujawnienie danych jest wyraźnie przewidziane prawem, lub
   c) poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
   d) dane objęte są tajemnicą zawodową przewidzianą w prawie;
   e) przetwarzanie danych, w tym ich upublicznienie, jest związane z pełnieniem funkcji duchownego lub ubieganiem się o niego, pełnieniem urzędu lub funkcji w Kościele lub jednostkach organizacyjnych Kościoła (z wyboru lub mianowania) – w zakresie bezpośrednio związanym z pełnieniem danego urzędu lub funkcji lub wynikającym z utrwalonego zwyczaju kościelnego, o ile nie narusza to godności takiej osoby;
4. Sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań

naukowych lub historycznych lub celom statystycznym, przy czym administrator zobowiązany jest podjąć odpowiednie środki ochrony danych.

§ 7

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora danych potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: a) cele przetwarzania;
   b) kategorie odnośnych danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do organu nadzorczego;
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.
2. Na zgłoszone żądanie, administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu, w tym poprzez sporządzenie wyciągu lub odpisu dokumentu, który zawiera dane takiej osoby, o ile nie naruszy praw i wolności innych osób, w tym poprzez ujawnienie w ten sposób danych innych osób bądź tajemnicy zawodowej. Za wszelkie kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
3. W przypadku, gdy osoba żądająca dostępu do jej danych zgłasza ustne żądanie w zakresie dostępu do tych danych, za zgodą osoby żądającej informacji, można poprzestać na ustnym udzieleniu informacji, o których mowa w ustępie powyżej.
4. Jeżeli dane osobowe są przekazywane do administratora w innym państwie lub organizacji międzynarodowej, której Kościół jest członkiem, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach danych osobowych związanych z przekazaniem.

§ 8

1. Osoba, której dane dotyczą, ma prawo żądania od administratora sprostowania jej danych osobowych, które są nieprawidłowe.
2. Osoba, której dane dotyczą, ma prawo żądania od administratora uzupełnienia jej danych osobowych, z uwzględnieniem celów przetwarzania jej danych osobowych.
3. Osoba żądająca sprostowania lub uzupełnienia danych, wnosi żądanie do administratora danych na piśmie, wskazując jednocześnie swój adres do doręczeń na potrzeby postępowania o sprostowanie lub uzupełnienie danych.
4. W przypadku gdy żądanie sprostowania lub uzupełnienia danych budzi wątpliwości, w tym m.in. jest nieprecyzyjne bądź zachodzą inne wątpliwości w zakresie złożonego żądania, administrator

wzywa osobę żądającą sprostowania lub uzupełnienia do uzupełnienia żądania lub złożenia dodatkowych wyjaśnień, zakreślając jej odpowiedni termin.

5. Administrator w terminie 14 dni od otrzymania żądania o sprostowanie lub uzupełnienie danych lub od otrzymania dodatkowych wyjaśnień, których mowa w ustępie powyżej dokonuje sprostowania lub uzupełnienia danych lub odmawia sprostowania lub uzupełnienia danych oraz wysyła informację o wyniku postępowania o sprostowanie lub uzupełnienie danych osobie, która żądała sprostowania lub uzupełnienia danych.
6. Sprostowanie lub uzupełnienie może nastąpić poprzez adnotację, stanowiącą integralną część dokumentu lub zbioru którego dotyczy. W przypadku gdy sprostowanie lub uzupełnienie miałoby wpływ na treść zapisów w księgach metrykalnych, administrator może wymagać dodatkowych dokumentów lub oświadczeń potwierdzających zasadność dokonania sprostowania lub uzupełnienia.
7. Administrator ma prawo odmowy sprostowania, jeżeli osoba żądająca sprostowania jej danych nie wykazała zasadności jej żądania.
8. Administrator może odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych.

§ 9

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych („prawo do bycia zapomnianym”), a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych i jednocześnie nie ma innej podstawy prawnej przetwarzania;
    c) osoba, której dane dotyczą, wniosła skuteczny w rozumieniu Rozporządzenia sprzeciw wobec przetwarzania;
    d) dane osobowe były przetwarzane niezgodnie z prawem;
    e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego.
2. Osoba żądająca usunięcia jej danych, wnosi żądanie do administratora danych na piśmie, wskazując jednocześnie swój adres do doręczeń na potrzeby postępowania o usunięcie jej danych osobowych.
3. Administrator niezwłocznie, nie później niż w terminie 14 dni od otrzymania żądania o usunięcie danych usuwa dane zgodnie z żądaniem, chyba że zachodzą podstawy wyłączające obowiązek usunięcia danych.
4. Administrator informuje osobę żądającą usunięcia danych, na adres podany na potrzeby postępowania o usunięcie danych, o usunięciu jej danych lub o odmowie usunięcia jej danych podając przyczynę odmowy usunięcia danych.
5. Administrator ma prawo odmówić usunięcia danych w przypadku, gdy:
    a) dane zostały zebrane w związku z wypełnianymi funkcjami statutowymi, w szczególności gdy dotyczą udzielonych sakramentów;

b) przetwarzanie jest niezbędne do korzystania z prawa do swobody wypowiedzi i wolności informacji, do wywiązania się z obowiązku prawnego lub do wykonania zadania realizowanego w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi lub ustalenia, dochodzenia lub obrony roszczeń;

c) dane wykorzystywane są do celów archiwalnych lub statystycznych, badań naukowych lub historycznych, o ile prawdopodobne jest, że prawo do zapomnienia uniemożliwi lub istotnie utrudni realizację takich celów.

6. W przypadku określonym w ust. 5 pkt a) przetwarzanie danych osobowych powinno zostać ograniczone do przechowywania danych, o ile nie naruszy to praw osób trzecich, interesu osoby, której dane dotyczą.

§ 10

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba wniosła sprzeciw wobec przetwarzania zgodnie z Rozporządzeniem.

2. W trakcie ograniczenia przetwarzania danych administrator przechowuje dane, natomiast nie wykorzystuje ich i nie przekazuje bez zgody osoby, której dotyczą.

3. Przepis § 9 ust. 5 i 6 stosuje się odpowiednio.

§ 11

1. W przypadku sprostowania, ograniczenia lub usunięcia danych, administrator jest zobowiązany powiadomić o tym administratorów danych, którym przekazał dane w ramach struktur Kościoła lub poza struktury Kościoła, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

2. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

3. Przepis ust. 2 nie ma zastosowania, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

4. W przypadkach określonych w ust. 3 administrator powinien wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa

do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

Rozdział IV

Zarządzanie ochroną danych

§ 12

1. Administrator ma obowiązek zapewnić odpowiednie środki organizacyjne i techniczne w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych, w tym postanowień niniejszego Regulaminu.
2. Na etapie projektowania oraz w trakcie procesów przetwarzania administrator powinien zastosować odpowiednie środki techniczne i organizacyjne, służące ochronie danych, a także pozwalające, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu przetwarzania.

§ 13

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, który obejmuje:
   a) nazwę administratora (lub współadministratorów) oraz jego dane kontaktowe, jak również inspektora ochrony danych, jeśli został powołany;
   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.
2. Procesy przetwarzania danych powinny być identyfikowalne i pogrupowane według celów przetwarzania danych.
3. Administrator ma obowiązek udostępnienia rejestru na żądanie organu nadzorczego.

§ 14

1. Administrator jest obowiązany powołać inspektora ochrony danych, jeżeli główna działalność administratora polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.
2. Administratorzy lub Święty Sobór Biskupów PAKP lub Biskupi Diecezjalni mogą powołać jednego inspektora ochrony danych dla większej liczby administratorów z uwzględnieniem struktury organizacyjnej Kościoła, w tym m.in. jednego inspektora ochrony danych dla wszystkich administratorów w danej diecezji.

3. Inspektor danych osobowych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych osobowych oraz umiejętności wykonywania zadań przewidzianych w Rozporządzeniu.
4. Na inspektora ochrony danych może zostać wybrana osoba będąca członkiem personelu, pracownikiem, współpracownikiem administratora lub podmiotu przetwarzającego.
5. Dane kontaktowe inspektora danych osobowych administrator publikuje na swojej stronie internetowej oraz udostępnia w miejscu dostępnym dla osób, których dane są przetwarzane.
6. O powołaniu i odwołaniu inspektora danych osobowych należy powiadomić organ nadzorczy ze wskazaniem dla jakich podmiotów został wyznaczony.

§ 15

1. Inspektor ochrony danych powinien być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Inspektor ochrony danych pełni funkcję doradczą dla administratora lub administratorów, dla których został wyznaczony.
3. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących.
4. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy, co do wykonywania swoich zadań.
5. Inspektor ochrony danych może wykonywać inne zadania i obowiązki, przy czym nie powinny one powodować konfliktu interesów.

§ 16

1. Do zadań inspektora danych osobowych należy w szczególności:
   a) informowanie administratora, podmiotu przetwarzającego oraz osób przetwarzających dane osobowy w imieniu administratora o obowiązkach spoczywających na nich na mocy prawa o ochronie danych osobowych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania prawa o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego lub całego Kościoła w dziedzinie ochrony danych osobowych;
   c) współpraca z organem nadzorczym;
   d) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Inspektor ochrony danych wypełnia swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 17

Administrator, inspektor ochrony danych oraz osoby przetwarzające dane osobowe w imieniu administratora:

a) współpracują z organem nadzorczym na jego żądanie w ramach wykonywania przez niego zadań własnych;

b) są zobowiązane do przekazywania organowi nadzorczemu wszelkich informacji i wyjaśnień, nieobjętych tajemnicą spowiedzi, o które zwróci się organ nadzoru w ramach swoich uprawnień – w ciągu 7 dni od otrzymania wezwania drogą korespondencyjną lub elektroniczną;

c) udostępniają zbiory danych, dokumenty oraz pomieszczenia do kontroli przez organ nadzoru – w ciągu 7 dni od otrzymania wezwania drogą korespondencyjną lub elektroniczną;

d) stosują się do zaleceń oraz rozstrzygnięć organu nadzoru - niezwłocznie bądź we wskazanym przez organ nadzoru terminie.

§ 18

1. W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z prawem administrator powinien oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.
2. Gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, administrator zobowiązany jest do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy uzyskać opinię organu nadzoru.
3. 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.

§ 19

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 ust. 1, musi co najmniej:
   a) 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;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) 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. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania przepisów w zakresie ochrony danych osobowych.
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 ust. 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.

Rozdział V

Organ nadzoru i rozpatrywanie skarg

§ 20

1. Kościelny Inspektor Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego (KIODO PAKP) jest organem właściwym w sprawie ochrony danych osobowych.
2. KIODO PAKP jest organem nadzorczym w rozumieniu 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. KIODO PAKP jest organem nadzorczym w zakresie w jakim przetwarza dane osobowe, niezależnie od tego czy przetwarzanie danych osobowych dotyczy

członków Kościoła, osób utrzymujących kontakty z Kościołem, czy też osób niebędących członkami Kościoła i niezwiązanych z Kościołem, których dane są przetwarzane w jednym lub większej liczbie określonych celów.

3. KIODO PAKP powoływany jest przez Św. Sobór Biskupów Kościoła na 5 letnią kadencję, liczoną od dnia powołania. Ta sama osoba może pełnić funkcję KIODO PAKP nieograniczoną liczbę kadencji.
4. Św. Sobór Biskupów może powołać od 1 do 3 zastępców KIODO PAKP pełniących funkcje pomocniczą i doradczą dla KIODO PAKP. Zastępcy KIODO PAKP powoływani są na 5 letnią kadencję, liczoną od dnia powołania. Ta sama osoba może pełnić funkcję Zastępcy KIODO PAKP nieograniczoną liczbę kadencji.
5. Kandydat na KIODO PAKP oraz na Zastępcę KIODO PAKP powinien:
    - posiadać wiedzę w zakresie ochrony danych osobowych,
    - posiadać wiedzę na temat specyfiki działania Kościoła oraz Kościelnych jednostek organizacyjnych w stopniu wystarczającym do realizacji obowiązków z zakresu ochrony danych osobowych,
    - wyrazić zgodę na pełnienie funkcji KIODO PAKP lub jego zastępcy.
6. Kandydatów na KIODO PAKP oraz jego zastępców może przedstawiać Św. Soborowi Biskupów Prawosławny Metropolita Warszawski i Całej Polski oraz członkowie Św. Soboru Biskupów. 7. W przypadku czasowej niemożności pełnienia funkcji KIODO PAKP, jego obowiązki przejmuje Zastępca KIODO PAKP wskazany przez Św. Sobór Biskupów, a w przypadku braku powołania Zastępcy KIODO PAKP, Św. Sobór Biskupów dokonuje niezwłocznego wyboru Zastępcy KIODO PAKP.
8. KIODO PAKP, jak również Zastępcy KIODO PAKP mogą złożyć rezygnację z pełnienia swoich funkcji. Rezygnacja jest skuteczna z chwilą przyjęcia jej przez Św. Sobór Biskupów.
9. KIODO PAKP, jak również Zastępcy KIODO PAKP mogą zostać odwołani uchwałą Św. Soboru Biskupów w przypadku niewywiązywania się z obowiązków nałożonych na organ nadzorczy Rozporządzeniem jak również w przypadku nieprawidłowego wykonywania obowiązków nałożonych na organ nadzorczy Regulaminem.

§ 21

1. Siedziba KIODO PAKP znajduje się w Warszawskiej Metropolii Prawosławnej.
2. Obsługę administracyjną organu nadzoru prowadzi Kancelaria Św. Soboru Biskupów.

§ 22

1. KIODO PAKP, jak również Zastępcy KIODO PAKP w przypadku ich powołania, podczas wypełniania swoich zadań związanych z ochroną danych osobowych są w pełni niezależni, wolni od bezpośrednich i pośrednich wpływów zewnętrznych
2. KIODO PAKP, jak również Zastępcy KIODO PAKP ma obowiązek zachowania tajemnicy służbowej w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień.
3. KIODO PAKP, jak również Zastępcy KIODO PAKP mogą otrzymywać zwrot uzasadnionych kosztów poniesionych w związku z wykonywaniem swoich obowiązków.

§ 23

1. Każda osoba, której dane dotyczą, ma prawo wnieść do organu nadzorczego skargę, jeżeli uważa, że przetwarzanie jej danych osobowych przez administratora będącego jednostką organizacyjną Kościoła narusza przepisy o ochronie danych osobowych, w tym przepisy Rozporządzenia.
2. Skarga wnoszona jest pisemnie do organu nadzorczego: Kościelny Inspektor Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego.
3. Organ nadzorczy może zwrócić się do skarżącego o uzupełnienie skargi lub dodatkowe wyjaśnienia niezbędne do rozpatrzenia skargi w zakresie naruszenia ochrony danych osobowych, wyznaczając skarżącemu termin na uzupełnienie skargi lub złożenie dodatkowych wyjaśnień.
4. W toku postępowania organ nadzorczy zapoznaje się z materiałem dowodowym, skargą, wyjaśnieniami skarżącego oraz stanowiskiem administratora danych. Organ nadzorczy może przeprowadzić dowód ze świadków jeśli jest to niezbędne do wyjaśnienia sprawy.
5. Rozpatrzenie skargi powinno nastąpić w terminie 30 dni od doręczenia skargi lub w terminie 30 dni od uzupełnienia skargi lub złożenia dodatkowych wyjaśnień, o których mowa powyżej. W wyjątkowych i skomplikowanych sprawach organ nadzorczy może przedłużyć czas rozpatrzenia skargi, informując o tym skarżącego.
6. Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzania może spowodować poważne i trudne do usunięcia skutki, organ nadzorczy, w celu zapobieżenia tym skutkom, może zobowiązać podmiot, któremu zarzucane jest naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych, wskazując dopuszczalny zakres tego przetwarzania.
7. Postępowanie przed organem nadzorczym kończy się rozstrzygnięciem o stwierdzeniu naruszenia zasad ochrony danych osobowych lub stwierdzeniem braku naruszenia zasad ochrony danych osobowych. W przypadku stwierdzenia naruszenia danych osobowych przez administratora, organ nadzorczy zobowiązuje administratora do określonego działania. Postępowanie przed organem nadzorczym jest postępowaniem jednoinstancyjnym.

§ 24 1.

Organ nadzoru wykonuje następujące zadania:

a) monitoruje i egzekwuje stosowanie prawa o ochronie danych osobowych;
b) upowszechnia w Kościele wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk;
c) doradza władzom Kościoła w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;
d) upowszechnia wśród administratorów danych wiedzę o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych;
e) udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących im na mocy prawa o ochronie danych osobowych;

f) rozpatruje skargi wniesione przez osobę, której dane dotyczą, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem;

g) prowadzi postępowania w sprawie stosowania prawa o ochronie danych osobowych, w tym na podstawie informacji otrzymanych od innego organu;

h) monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych;

i) prowadzi wewnętrzny rejestr naruszeń prawa o ochronie danych osobowych;

j) wypełnia inne zadania związane z ochroną danych osobowych, w tym wydaje zalecenia dla administratorów i władz kościelnych.

2. Organ nadzoru może delegować wykonywanie zadań i obowiązków, o których mowa powyżej swoim Zastępcom.

§ 25 Organowi

nadzoru przysługują następujące uprawnienia:

a) uzyskiwanie od administratora lub osoby odpowiedzialnej dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań;

b) uzyskiwanie dostępu do wszystkich pomieszczeń administratora, w tym do sprzętu i środków służących do przetwarzania danych;

c) wydawanie ostrzeżeń administratorowi lub osobie odpowiedzialnej dotyczących możliwości naruszenia przepisów poprzez planowane operacje przetwarzania;

d) udzielanie upomnień administratorowi lub osobie odpowiedzialnej w przypadku naruszenia przepisów przez operacje przetwarzania;

e) nakazanie administratorowi lub osobie odpowiedzialnej spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy prawa o ochronie danych osobowych;

f) nakazanie administratorowi lub osobie odpowiedzialnej dostosowania operacji przetwarzania do przepisów prawa o ochronie danych osobowych, a w stosownych przypadkach wskazanie sposobu i terminu;

g) nakazanie administratorowi lub osobie odpowiedzialnej zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;

h) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

i) nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

j) kierowanie wniosku o rozpoczęcie procedury dyscyplinarnej do Biskupa Diecezjalnego lub Św. Soboru Biskupów;

k) wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla administratorów we wszelkich sprawach związanych z ochroną danych osobowych.

§ 26

Organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności i przedstawia je Św. Soborowi Biskupów.

§ 27

Niezależnie od zadań nałożonych na KIODO PAKP, do biskupa diecezjalnego, w ramach działań kontrolnych sprawowanych w danej diecezji, należy także nadzór nad prawidłowym przestrzeganiem powszechnie obowiązujących przepisów prawa dotyczących przetwarzania danych osobowych, w tym w szczególności przepisów Rozporządzenia oraz niniejszego Regulaminu.

§ 28

1. Naruszenie prawa o ochronie danych osobowych może stanowić wykroczenie dyscyplinarne, szczególnie gdy osoba, której dane zostały naruszone, poniosła szkodę.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych, organ nadzorczy może skierować wniosek do Biskupa Diecezjalnego lub Św. Soboru Biskupów o wszczęcie postępowania dyscyplinarnego.
3. W przypadku wszczęcia postępowania dyscyplinarnego, Biskup Diecezjalny lub Św. Sobór Biskupów informuje organ nadzorczy o wszczęciu postępowania dyscyplinarnego, jak również o wyniku postępowania dyscyplinarnego.

Rozdział VI

Przepisy przejściowe i końcowe

§ 29

1. W zakresie nieuregulowanym należy odpowiednio stosować przepisy Rozporządzenia.
2. Regulamin wchodzi w życie z dniem promulgacji.
3. Promulgacja niniejszego Regulaminu następuje przez publikację.