Dekret ogólny
w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim

**wydany przez Konferencję Episkopatu Polski, w dniu 13 marca 2018 r.,
podczas 378. Zebrania Plenarnego w Warszawie,
na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP,
po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r.**

Chrześcijaństwo wniosło do kultury europejskiej przekonanie o nienaruszalnej godności osoby ludzkiej. Zakorzenione ono jest w fakcie stworzenia człowieka na „obraz i podobieństwo" Boga. Godność jest przymiotem ludzkiej natury rozumnej i wolnej. Uznanie godności człowieka wymaga odpowiedniej ochrony danych osobowych.

Biorąc pod uwagę zasady ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych stosowane dotychczas w Kościele katolickim w Polsce, a zwłaszcza mając na uwadze:

- kan. 220 Kodeksu Prawa Kanonicznego oraz kan. 23 Kodeksu Kanonów Kościołów Wschodnich, gwarantujące prawo do dobrego imienia i prawo do ochrony intymności,
- kan. 482-491 i kan. 535 Kodeksu Prawa Kanonicznego oraz kan. 252-261 i kan. 296 Kodeksu Kanonów Kościołów Wschodnich, zobowiązujące każdą parafię do prowadzenia ksiąg parafialnych, zgodnie z przepisami Konferencji Biskupów i biskupa diecezjalnego oraz zobowiązujące proboszcza do ich właściwego sporządzania i przechowywania oraz dotyczące obowiązku posiadania archiwum przez kurie diecezjalne i parafie, i zasad ich prowadzenia,
- kan. 1067 i 1069 Kodeksu Prawa Kanonicznego oraz kan. 784 i 786 Kodeksu Kanonów Kościołów Wschodnich, dotyczące kanonicznego przygotowania do małżeństwa, a w szczególności przekazywania informacji o okolicznościach mających znaczenie dla możliwości jego zawarcia,
- Motu proprio *La cura vigilantissima* z dnia 21 marca 2005 r. (AAS 97(2005), s. 353-376),
- Przepisy Konferencji Episkopatu Polski o prowadzeniu ksiąg parafialnych: ochrzczonych, bierzmowanych, małżeństw i zmarłych, oraz księgi stanu dusz z dnia 26 października 1947 r.,
- Instrukcję opracowaną przez Generalnego Inspektora Ochrony Danych Osobowych oraz Sekretariat Konferencji Episkopatu Polski z dnia 23 września 2009 r. „Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce",
- Dekret Ogólny Konferencji Episkopatu Polski w sprawie wystąpień z Kościoła oraz powrotu do wspólnoty Kościoła z dnia 7 października 2015 r.,
- oraz inne regulacje prawa partykularnego,

przypominając powszechnie uznaną zasadę autonomii państwa i Kościoła,

mając na względzie konieczność pogodzenia ochrony danych osobowych z korzystaniem z podstawowego prawa do wolności religijnej, zagwarantowanego również w prawie pozytywnym, także w jego wymiarze instytucjonalnym,

działając w celu uszczegółowienia przepisów Kodeksu Prawa Kanonicznego i uaktualnienia przepisów prawa partykularnego,

postanawia się, co następuje:

Rozdział I
Zagadnienia ogólne

Art. 1 – Przedmiot regulacji

Niniejszy dekret określa szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim w Polsce.

Art. 2 – Odesłanie do innych przepisów prawa kanonicznego

Zasady redagowania, zarządzania oraz nadzoru nad zbiorami danych, a także wykorzystywania danych, są określone przez przepisy powszechnego oraz partykularnego prawa kanonicznego, uzupełniane w razie potrzeby przez przepisy wydane przez Konferencję Episkopatu Polski.

Art. 3 – Zakres przedmiotowy

Niniejszy dekret ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Art. 4 – Zakres podmiotowy

Niniejszy dekret stosuje się do publicznych kościelnych osób prawnych.

Art. 5 – Słowniczek pojęć

Na potrzeby niniejszego dekretu:

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, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

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; w działalności Kościoła zbiorami danych są w szczególności: księgi parafialne zawierające rejestr ochrzczonych, bierzmowanych, Pierwszej Komunii świętej, zawartych małżeństw, zgonów, jak również rejestr parafian, alumnów seminariów duchownych, nowicjuszy i członków instytutów życia konsekrowanego i stowarzyszeń życia apostolskiego;

4) „administrator” oznacza osobę prawną lub inną jednostkę organizacyjną, która 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) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, bądź jednostkę organizacyjną, której ujawnia się dane osobowe. Organy publiczne, które mogą otrzymywać

dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są jednak uznawane za odbiorców;

7) „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;

8) „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;

9) „dane wrażliwe" oznaczają dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne a także dane dotyczące zdrowia lub seksualności osoby fizycznej;

10) „dane genetyczne" oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

11) „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak np. wizerunek twarzy lub dane daktyloskopijne;

12) „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

Rozdział II
Zasady przetwarzania danych

Art. 6 – Standardy przetwarzania danych

1. Dane osobowe powinny być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;

2) zbierane w konkretnych, wyraźnych 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;

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

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

5) 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, do celów badań naukowych lub historycznych albo do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą;

6) 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.

2. Za przestrzeganie określonych powyżej zasad odpowiedzialny jest administrator, który powinien być w stanie wykazać ich przestrzeganie. Na administratorze spoczywa obowiązek czuwania nad prawidłowym zachowaniem przedmiotowych norm kanonicznych oraz koordynacji działalności ewentualnych współpracowników.

Art. 7 – Dopuszczalność przetwarzania danych

1. W działalności publicznych kościelnych osób prawnych przetwarzanie danych osobowych jest dopuszczalne, jeżeli:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

2) 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;

3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, zgodnie z przepisami prawa kanonicznego lub prawa świeckiego;

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

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

6) 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. Przetwarzanie danych wrażliwych dopuszczalne jest wyłącznie w stosunku do osób ochrzczonych w Kościele katolickim i tych, którzy po chrzcie zostali do niego przyjęci (członków Kościoła), łącznie z tymi, którzy złożyli formalne oświadczenie woli o wystąpieniu z Kościoła katolickiego, zgodnie z wewnętrznymi przepisami Kościoła („byłych członków Kościoła") oraz osób utrzymujących z nim stałe kontakty w związku z realizacją celów Kościoła w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń. Dane te nie są ujawniane poza Kościołem bez zgody osób, których dane dotyczą.

Art. 8 – Informowanie o przetwarzaniu danych w przypadku zbierania danych od osoby, której dane dotyczą

1. W przypadku zbierania danych od osoby, której dane dotyczą, administrator danych informuje tę osobę o przetwarzaniu, podając informacje identyfikujące administratora i pozwalające się z nim skontaktować, bądź dane kontaktowe inspektora ochrony danych, wskazując cel przetwarzania danych, podstawę prawną przetwarzania, informacje o odbiorcach oraz zamiarze przekazania danych do publicznej kościelnej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej. Ponadto administrator podaje informacje o okresie przetwarzania danych, informacje o prawie do żądania od administratora dostępu do danych osobowych, prawie domagania się ich sprostowania, usunięcia lub ograniczenia przetwarzania zgodnie z niniejszym Dekretem, oraz informacje o prawie wniesienia skargi do Kościelnego Inspektora Ochrony Danych;

2. Przepis ust. 1 nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.

Art. 9 - Informowanie przy zbieraniu danych z innych źródeł

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, informacje wskazane w art. 8 ust. 1 oraz informacje o źródle pochodzenia danych. Przekazanie informacji powinno nastąpić w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze okoliczności przetwarzania danych osobowych.

2. Przepis ust. 1 nie ma zastosowania, gdy – i w zakresie, w jakim:

1) osoba, której dane dotyczą, dysponuje już tymi informacjami;

2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub

4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym obowiązkiem zachowania tajemnicy spowiedzi, zgodnie z kan. 983 § 1 Kodeksu Prawa Kanonicznego i kan. 773 § 1 Kodeksu Kanonów Kościołów Wschodnich, tajemnicy, o której mowa w kan. 983 § 2 Kodeksu Prawa Kanonicznego i kan. 773 § 2 Kodeksu Kanonów Kościołów Wschodnich oraz tajemnicy duszpasterskiej.

Art. 10 - Publikacja periodyków urzędowych

1. Roczniki (informatory, schematyzmy, itp.) jako użyteczne narzędzia do wykonywania zadań instytucjonalnych kościelnych publicznych osób prawnych, wydawane są pod ich własną redakcją i zawierają dane niezbędne do określenia organów, urzędów, struktur, osób uprawnionych do ich reprezentacji i personelu pomocniczego.

2. Periodyki informacyjne przeznaczone do użytku wewnętrznego, opisujące najważniejsze wydarzenia z życia i działalności redagujących je podmiotów kościelnych, mogą zawierać dane dotyczące osób uczestniczących w uroczystościach i wydarzeniach oraz dane dotyczące osób, które złożyły darowiznę, o ile w poszczególnych przypadkach zainteresowani nie wnosili o ich nieujawnianie.

3. Zasady zawarte w ust. 1 i 2 stosuje się odpowiednio do publikacji cyfrowych i stron internetowych.

Rozdział III
Prawa osoby, której dane dotyczą

Art. 11 - Prawo do informacji o przetwarzaniu danych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz do otrzymania następujących informacji:

1) cele przetwarzania;

2) kategorie odnośnych danych osobowych;

3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;

4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, zgodnie z niniejszym Dekretem;

6) informacje o prawie wniesienia skargi do Kościelnego Inspektora Ochrony Danych;

7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – informacje o ich źródle.

2. Jeżeli dane osobowe są przekazywane do publicznej kościelnej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, związanych z przekazaniem.

3. Administrator, ma obowiązek, na żądanie osoby, której dane dotyczą, dostarczyć jej kopię danych podlegających przetwarzaniu.

4. Każdy ma prawo do żądania i otrzymania, osobiście lub za pośrednictwem prawnie ustanowionego pełnomocnika, certyfikatów, wyciągów, świadectw, w postaci kopii lub dokumentu autentycznego, zawierających dane jego dotyczące. Wyłączeniu podlegają dane, które jako nie pochodzące od wnioskodawcy, są objęte tajemnicą na mocy prawa lub nie można ich oddzielić od danych dotyczących osób trzecich i ze względu na poufność wymagają ochrony.

5. Za wystawienie dokumentów, o których mowa w ust. 4, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Prawo pobrania opłaty dotyczy również kolejnych kopii danych osobowych podlegających przetwarzaniu, sporządzonych na wniosek osoby, której dane dotyczą po zrealizowaniu przez administratora obowiązku określonego w ust. 3.

Art. 12 - Prawo do żądania sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, jeżeli dane są nieprawidłowe.

2. Wniosek o sprostowanie danych powinien zostać przedstawiony w formie pisemnej administratorowi, osobiście lub za pośrednictwem prawnie ustanowionego pełnomocnika, z załączeniem właściwych dokumentów, w razie potrzeby także cywilnych.

3. Jeżeli administrator odmówi przyjęcia wniosku o sprostowanie danych, powinien pisemnie powiadomić o odmowie wnioskodawcę, który będzie mógł złożyć ponownie wniosek do ordynariusza miejsca lub wyższego przełożonego instytutu życia konsekrowanego lub stowarzyszenia życia apostolskiego.

4. Sprostowanie danych dotyczących aktów i faktów dotyczących stanu kanonicznego osoby może zostać dokonane jedynie za zezwoleniem ordynariusza miejsca lub wyższego przełożonego instytutu życia konsekrowanego lub stowarzyszenia życia apostolskiego.

Art. 13 – Prawo do żądania dokonania adnotacji i uzupełnienia danych

1. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo w uzasadnionym zakresie żądać umieszczenia w zbiorze danych adnotacji lub uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2. Wniosek o dokonanie adnotacji lub uzupełnienie danych powinien spełniać warunki określone w art. 12 ust. 2.

3. Adnotacja dokonana na marginesie dokumentu stanowi jego część integralną. Jej treść winna być umieszczona w każdym wyciągu lub kopii aktu.

4. Administrator powiadamia pisemnie wnioskodawcę o dokonanej adnotacji.

5. W przypadku odrzucenia wniosku, zostaje on odnotowany i przechowywany w aneksie do właściwego zbioru. Administrator powiadamia na piśmie o odrzuceniu wniosku zainteresowanego, który może ponownie złożyć wniosek do ordynariusza miejsca lub wyższego przełożonego instytutu życia konsekrowanego lub stowarzyszenia życia apostolskiego.

Art. 14 – Prawo do żądania usunięcia danych

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych, i nie ma innej podstawy prawnej przetwarzania;

3) dane osobowe były przetwarzane niezgodnie z prawem.

2. Jeżeli administrator upublicznił dane osobowe, a ma obowiązek ich usunięcia, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

3. Zasady, o których mowa w ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

1) do korzystania z prawa do swobody wypowiedzi i wolności informacji;

2) do wywiązania się z obowiązku prawnego wymagającego przetwarzania lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;

4) do ustalenia, dochodzenia lub obrony roszczeń.

4. Prawo do żądania usunięcia danych nie przysługuje w przypadku, gdy dane dotyczą udzielonych sakramentów bądź w inny sposób odnoszą się do kanonicznego statusu osoby. Tego typu wniosek powinien zostać odnotowany w zbiorze i zobowiązuje administratora do niewykorzystywania danych objętych wnioskiem bez zgody ordynariusza miejsca lub wyższego przełożonego instytutu życia konsekrowanego lub stowarzyszenia życia apostolskiego.

Art. 15 – Prawo do żądania ograniczenia przetwarzania

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

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

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

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

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą,

lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

Art. 16 - Obowiązek powiadomienia

Administrator informuje każdego odbiorcę, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Rozdział IV
Administrator i podmiot przetwarzający

Art. 17 – Obowiązki administratora

1. Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Administrator jest zobowiązany do przestrzegania przepisów kanonicznych dotyczących starannego przechowywania, dozwolonego użytku i właściwego zarządzania danymi osobowymi.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Zarówno na etapie projektowania, jak też 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.

Art. 18 – Współadministratorzy

1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swoich obowiązków i odpowiedzialności.

2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wobec każdego z współadministratorów.

Art. 19 – Powierzenie przetwarzania i obowiązki podmiotu przetwarzającego

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora przez podmiot przetwarzający, podmiot ten powinien zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego dekretu i gwarantowało ochronę praw osób, których dane dotyczą.

2. Przetwarzanie danych przez podmiot przetwarzający powinno opierać się na umowie lub innym zobowiązaniu prawnym ustalającym zakres odpowiedzialności i procedury, gwarantującym, że podmiot przetwarzający:

1) będzie przetwarzał dane wyłącznie w zakresie i celu określonym w umowie;

2) zapewni, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy;

3) podejmie środki wymagane w celu zabezpieczenia danych;

4) będzie pomagał administratorowi wypełniać obowiązki w zakresie informowania osób, których dane dotyczą, realizowania ich uprawnień oraz obowiązki dotyczące zawiadamiania o naruszeniach;

5) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usunie lub zwróci mu wszelkie dane osobowe oraz usunie wszelkie ich istniejące kopie;

6) udostępni administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwi administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.

3. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora.

4. Powierzenie przetwarzania danych podmiotowi nie należącemu do porządku kanonicznego musi zostać dokonane na podstawie umowy zawartej zgodnie z kan. 1290 Kodeksu Prawa Kanonicznego i kan. 1034 Kodeksu Kanonów Kościołów Wschodnich, z zastrzeżeniem, że także na podmiocie, któremu zostają powierzone dane spoczywa obowiązek zachowania przepisów niniejszego dekretu.

Art. 20 – Przetwarzanie z upoważnienia. Obowiązek zachowania tajemnicy

1. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo.

2. Administrator oraz każda inna osoba posiadająca stały dostęp do danych gromadzonych przez podmioty kościelne lub przez nie prawnie nabytych, jest zobowiązana do zachowania tajemnicy dotyczącej wszystkich przetwarzanych danych osobowych. Obowiązek zachowania tajemnicy pozostaje nienaruszony także po zakończeniu pełnienia funkcji.

Art. 21 - Rejestrowanie czynności przetwarzania

1. Każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się następujące informacje:

1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz współadministratorów, a także gdy ma to zastosowanie – inspektora ochrony danych;

2) cele przetwarzania;

3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;

5) gdy ma to zastosowanie, informacje o przekazywaniu danych do publicznej kościelnej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej;

6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

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

2. Każdy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

1) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – inspektora ochrony danych;

2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

3) gdy ma to zastosowanie – przekazania danych osobowych do publicznej kościelnej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej;

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

3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym elektroniczną.

4. Administrator lub podmiot przetwarzający udostępniają rejestr na żądanie Kościelnego Inspektora Ochrony Danych.

Art. 22 – Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo.

Art. 23 – Warunki przechowywania zbiorów danych

1. Zbiory danych powinny być przechowywane w pomieszczeniu przeznaczonym do tego celu, bezpiecznym, należącym lub dostępnym wyłącznie dla administratora, podmiotu przetwarzającego oraz osób przetwarzających na podstawie upoważnienia.

2. W przypadku braku pomieszczenia o takich właściwościach, powinny być one przechowywane w szafie umieszczonej w lokalu należącym do administratora lub podmiotu przetwarzającego na zlecenie administratora lub dostępnym wyłącznie im i osobom przez nich upoważnionym, z wystarczającą gwarancją ich bezpieczeństwa i nienaruszalności.

Art. 24 – Przechowywanie danych w archiwach

1. Szczególną uwagę należy zwrócić na zapewnienie nienaruszalności archiwów i ich zarządzanie.

2. Archiwum powinno być wyposażone w system zamknięcia, który gwarantuje wystarczającą ochronę przed kradzieżą i włamaniem.

3. Klucze do archiwum winny być starannie przechowywane przez administratora danych lub osobę przez niego upoważnioną. Staranność powinna być dochowana także przy autoryzacji dostępu udzielanego osobom postronnym.

Art. 25 – Przechowywanie danych w archiwach cyfrowych

1. Dane zawarte w archiwach cyfrowych winny być zarządzane za pomocą licencjonowanego oprogramowania, pozwalającego na kontrolę dostępu przy pomocy systemu identyfikatorów i haseł dostępu.

2. Administrator winien zapewnić bezpieczeństwo danych poprzez okresowo dokonywany ich zapis i przeniesienie na inne nośniki, zabezpieczone przed dostępem osób postronnych.

3. Urządzenia i nośniki zawierające dane winny być przechowywane w pomieszczeniach zamkniętych i zabezpieczonych przed dostępem osób nieuprawnionych.

Art. 26 – Tajne archiwum

Tajne archiwum, ustanowione na podstawie ogólnych przepisów kanonicznych winno być strzeżone z uwzględnieniem jego szczególnego charakteru, zgodnie z przepisami kan. 489-490 Kodeksu Prawa Kanonicznego i kan. 259-260 Kodeksu Kanonów Kościołów Wschodnich oraz odpowiednimi przepisami partykularnymi, w tym obowiązującymi w instytutach życia konsekrowanego i stowarzyszeniach życia apostolskiego.

Art. 27 – Zgłaszanie naruszenia ochrony danych osobowych Kościelnemu Inspektorowi Ochrony Danych

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Kościelnemu Inspektorowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

3. Zgłoszenie, o którym mowa w ust. 1, powinno co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną 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 ochrony danych 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.

4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki.

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna pozwolić Kościelnemu Inspektorowi Ochrony Danych na weryfikowanie przestrzegania niniejszego artykułu.

Art. 28 - Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 27 ust. 3 pkt 2-4.

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

1) administrator 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;

2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, Kościelny Inspektor Ochrony Danych – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

Art. 29 – Zgłoszenie naruszenia innym podmiotom

Niezależnie od spełnienia obowiązków określonych w art. 27-28, administrator winien zgłosić bezzwłocznie właściwej władzy kościelnej, a w razie potrzeby także organom ścigania, każde wtargnięcie do archiwum, lub do pomieszczenia, w którym przechowywane są zbiory danych, którego skutkiem była utrata lub zniszczenie rejestrów, akt, dokumentów urzędowych, indeksów i katalogów zawierających dane osobowe.

Art. 30 – Powołanie inspektora ochrony danych

1. Kościelna publiczna osoba prawna może wyznaczyć inspektora ochrony danych. W przypadku, gdy przetwarzanie danych odbywa się na dużą skalę, kościelna publiczna osoba prawna powinna wyznaczyć inspektora ochrony danych.

2. Kilka kościelnych publicznych osób prawnych może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Inspektor ochrony danych powinien być wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 32.

4. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

5. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich Kościelnego Inspektora Ochrony Danych.

Art. 31 – Status inspektora ochrony danych

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był 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 wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji, które uniemożliwiałyby mu wykonywanie jego zadań. Nie powinien on być odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega administratorowi lub podmiotowi przetwarzającemu.

4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego dekretu.

5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa kanonicznego lub świeckiego.

6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Art. 32 – Zadania inspektora ochrony danych

Do zadań inspektora ochrony danych należy:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach w zakresie ochrony danych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania niniejszego dekretu oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3) współpraca z Kościelnym Inspektorem Ochrony Danych;

4) pełnienie funkcji punktu kontaktowego dla Kościelnego Inspektora Ochrony Danych w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Art. 33 – Współpraca z organem nadzorczym

Administrator, podmiot przetwarzający i inspektor ochrony danych – jeśli został on wyznaczony – współpracują z Kościelnym Inspektorem Ochrony Danych w ramach wykonywania przez niego zadań.

Art. 34 – Przekazywanie danych i sporządzanie wypisów

1. Przekazanie danych do innego kościelnego zbioru danych może nastąpić na wniosek osoby, której dane dotyczą lub na wniosek administratora zbioru danych, w którym mają zostać użyte wnioskowane dane. Może to nastąpić poprzez dostarczenie bezpośrednie lub za pośrednictwem poczty lub – z zachowaniem ostrożności – drogą elektroniczną.

2. Przekazywanie danych osobowych przez kościelne publiczne osoby prawne innym podmiotom może nastąpić w przypadku, gdy:

1) jest to niezbędne dla wykonania zadań określonych w przepisach prawa;

2) osoba, której dane dotyczą została o tym poinformowana i uprzednio wyraziła zgodę na przekazanie danych w formie pisemnej;

3) przekazanie jest niezbędne dla wykonania umowy, której stroną jest osoba, której dane dotyczą lub w interesie której dane miałyby zostać przekazane;

4) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego.

3. Dokonanie wypisu i przekazanie danych zawartych w zbiorze poza przypadkami przewidzianymi w ust. 1 i 2 oraz w art. 11 ust. 4, jest ponadto dopuszczalne:

1) dla celów badawczych, z zachowaniem kryteriów metodologicznych i deontologicznych odnoszących się do badań historycznych, a w szczególności wskazanych w regulacjach dotyczących archiwów kościelnych;

2) dla celów statystycznych, po uprzednim usunięciu danych identyfikujących osoby.

Rozdział V
Kościelny Inspektor Ochrony Danych

Art. 35 – Niezależność Kościelnego Inspektora Ochrony Danych

1. Kościelny Inspektor Ochrony Danych jest niezależnym organem monitorującym i zapewniającym przestrzeganie przepisów o ochronie danych osobowych w ramach i zgodnie z działaniem Kościoła katolickiego i jego struktur. Kościelny Inspektor Ochrony Danych w zakresie wykonywania swoich zadań nadzorczych nie podlega poleceniom innych podmiotów.

2. Funkcja Kościelnego Inspektora Ochrony Danych jest urzędem w rozumieniu kan. 145 Kodeksu Prawa Kanonicznego.

3. Osoba pełniąca funkcję Kościelnego Inspektora Ochrony Danych ma obowiązek powstrzymać się od wszelkich zajęć i działań, niedających się pogodzić z pełnioną funkcją.

4. Konferencja Episkopatu Polski zapewnia warunki i środki niezbędne do skutecznego wypełniania zadań przez Kościelnego Inspektora Ochrony Danych.

Art. 36 – Wybór Kościelnego Inspektora Ochrony Danych

1. Kościelny Inspektor Ochrony Danych jest wybierany przez Zebranie Plenarne Konferencji Episkopatu Polski na czteroletnią kadencję. Ta sama osoba może być wybierana na kolejne kadencje.

2. Osoba pełniąca funkcję Kościelnego Inspektora Ochrony Danych powinna posiadać odpowiednią wiedzę, doświadczenie i umiejętności w zakresie ochrony danych osobowych, niezbędne do prawidłowego wypełniania swoich zadań.

3. Kościelny Inspektor Ochrony Danych może zostać odwołany z pełnionej funkcji tylko w przypadku, gdy dopuścił się poważnego uchybienia swoich obowiązków albo przestał spełniać wymogi niezbędne do pełnienia urzędu.

4. Kościelny Inspektor Ochrony Danych może złożyć rezygnację z pełnionego urzędu. Winna być ona złożona na piśmie i osiąga skutek z chwilą jej notyfikowania Przewodniczącemu Konferencji Episkopatu Polski.

Art. 37 – Zadania Kościelnego Inspektora Ochrony Danych

1. Do zadań Kościelnego Inspektora Ochrony Danych należy:

1) monitorowanie i zapewnianie przestrzegania przepisów o ochronie danych osobowych w ramach i zgodnie z działaniem Kościoła katolickiego i jego struktur;

2) upowszechnianie wiedzy o ochronie danych osobowych w Kościele;

3) doradzanie administratorom danych i podmiotom przetwarzającym w Kościele w zakresie ochrony danych osobowych;

4) udzielanie osobie, której dane dotyczą informacji dotyczących uprawnień przysługujących jej w związku z przetwarzaniem jej danych osobowych;

5) rozpatrywanie skarg dotyczących przestrzegania przepisów ustanowionych w Kościele w zakresie ochrony danych osobowych;

6) podejmowanie decyzji dotyczących dopuszczalności przekazywania danych do publicznej kościelnej osoby prawnej mającej siedzibę poza terytorium Rzeczypospolitej Polskiej, jeśli istnieją uzasadnione wątpliwości odnośnie do ochrony tych danych;

7) współpraca z krajowym organem nadzorczym, w tym dzielenie się informacjami oraz świadczenie wzajemnej pomocy w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych;

8) monitorowanie zmian w działalności Kościoła mających wpływ na ochronę danych osobowych, w szczególności stosowania technologii informacyjnych i komunikacyjnych;

9) przedkładanie Konferencji Episkopatu Polski propozycji regulacji prawnych bądź zmian regulacji dotyczących ochrony danych osobowych.

2. Kościelny Inspektor Ochrony Danych nie jest uprawniony do monitorowania i ingerencji w przekazywanie danych do Stolicy Apostolskiej.

3. Kościelny Inspektor Ochrony Danych nie może monitorować ani ingerować w przetwarzanie danych dokonywane przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości.

Art. 38 – Uprawnienia Kościelnego Inspektora Ochrony Danych

W celu realizacji zadań Kościelny Inspektor Ochrony Danych jest uprawniony do:

1) żądania od podmiotów przetwarzających dane osobowe w Kościele udzielenia informacji związanych z przetwarzaniem i ochroną danych;

2) przeprowadzenia kontroli działalności podmiotów przetwarzających dane osobowe w Kościele;

3) nakazania przywrócenia stanu zgodnego z prawem w przypadku stwierdzenia nieprawidłowości przy przetwarzaniu danych;

4) nakazania administratorowi poinformowania osoby, której dane dotyczą o naruszeniu ochrony danych;

5) podjęcia innych środków, niezbędnych do zapewnienia skutecznej ochrony danych osobowych w Kościele.

Art. 39 – Sprawozdanie z działalności Kościelnego Inspektora Ochrony Danych

Kościelny Inspektor Ochrony Danych sporządza roczne sprawozdanie ze swojej działalności, które jest przekazywane Konferencji Episkopatu Polski oraz publikowane w Aktach Konferencji Episkopatu Polski.

Art. 40 – Nadzór

1. Niezależnie od monitorowania i zapewniania przez Kościelnego Inspektora Ochrony Danych przestrzegania przepisów w zakresie ochrony danych osobowych w rozumieniu art. 35 ust. 1 niniejszego Dekretu, do biskupa diecezjalnego w ramach zwyczajnych działań kontrolnych (np. podczas wizytacji kanonicznych) należy także nadzór nad prawidłowym przestrzeganiem przepisów dotyczących pozyskiwania, przechowywania i przetwarzania danych osobowych.

2. W instytutach życia konsekrowanego i stowarzyszeniach życia apostolskiego nadzór, o którym mowa w ustępie poprzedzającym, sprawuje wyższy przełożony.

Rozdział VI
Procedura odwoławcza i odpowiedzialność za naruszenie przepisów niniejszego Dekretu ogólnego

Art. 41 – Procedura odwoławcza

Jeśli osoba, której dane dotyczą, uzna, że przetwarzanie danych nie jest zgodne z przepisami niniejszego Dekretu, może złożyć skargę do Kościelnego Inspektora Ochrony Danych, a następnie do właściwej dykasterii Stolicy Apostolskiej, zgodnie z przepisami Kodeksu Prawa Kanonicznego.

Art. 42 – Sankcje

1. Kto powoduje szkody materialne lub moralne poprzez nieuprawnione pozyskanie, przechowywanie i wykorzystywanie danych osobowych jest zobowiązany do naprawienia

szkody zgodnie z kan. 128 Kodeksu Prawa Kanonicznego oraz kan. 935 Kodeksu Kanonów Kościołów Wschodnich.

2. Karze przewidzianej przez kan. 1389 Kodeksu Prawa Kanonicznego oraz kan. 1464 Kodeksu Kanonów Kościołów Wschodnich podlega ten, kto naruszając niniejsze przepisy:

1) nadużywa władzy kościelnej lub urzędu;

2) dokona lub zaniecha bezprawnie z powodu zawinionego zaniedbania aktu władzy kościelnej lub aktu urzędowego powodując szkodę dla innej osoby.

3. Karą przewidzianą w kan. 1390 § 2 Kodeksu Prawa Kanonicznego oraz kan. 1452 Kodeksu Kanonów Kościołów Wschodnich może zostać ukarany ten, kto nie zachowując niniejszych przepisów narusza czyjeś dobre imię.

4. Jeżeli przestępstwo polega na naruszeniu obowiązku służbowego kara podlega zaostrzeniu i może także polegać na odwołaniu lub na pozbawieniu urzędu zgodnie z kan. 193 § 1 i 3; 196 § 1; 1336 § 1, n. 2° i 1389 Kodeksu Prawa Kanonicznego oraz kan. 975 § 1 i 2; 978; 1464 Kodeksu Kanonów Kościołów Wschodnich.

Rozdział VII
Przepisy końcowe

Art. 43 – Zasada swobody komunikacji

Kościół katolicki w Polsce, jego osoby prawne i fizyczne korzystają ze swobody utrzymywania stosunków i komunikowania się ze Stolicą Apostolską, z Konferencjami Biskupów, z Kościołami partykularnymi, a także między sobą i z innymi wspólnotami, instytucjami, organizacjami i osobami w kraju i za granicą. Żaden artykuł tego Dekretu nie może być interpretowany w sposób, który w istotnym stopniu ograniczałby tę swobodę.

Art. 44 – Wejście w życie

1. Niniejszy Dekret wchodzi w życie po uzyskaniu *recognitio* Stolicy Apostolskiej z chwilą promulgacji, zgodnie z kan. 455 § 2 i 3 w związku z kan. 8 § 2 Kodeksu Prawa Kanonicznego.

2. Promulgacja niniejszego Dekretu następuje poprzez zamieszczenie go na oficjalnej stronie internetowej Konferencji Episkopatu Polski.

\+ *Stanisław Gądecki*
Arcybiskup Metropolita Poznański
Przewodniczący KEP

\+ *Artur G. Miziński*
Sekretarz Generalny KEP