STUDIA WŁOCŁAWSKIE
26(2024), s. 391–404
10.52404/ttnwloc.stwl.26.19

KS. JANUSZ BORUCKI [a,b,@]
0000-0002-6055-2072
[a] Akademia Katolicka w Warszawie; Studium Teologii, ul. św. Maksymiliana 2, 62-510 Konin, wielkopolskie, PL
[b] Teologiczne Towarzystwo Naukowe Wyższego Seminarium Duchownego we Włocławku, ul. Prymasa Stanisława Karnkowskiego 3, 87-800 Włocławek, PL
[@] J.Borucki@ONet.PL

OCHRONA DANYCH OSOBOWYCH I ICH PRZETWARZANIA W KOŚCIELE KATOLICKIM W POLSCE

Słowa kluczowe: ochrona danych osobowych, dekrety ogólne Konferencji Episkopatu Polski, Kodeks prawa kanonicznego.

Streszczenie: W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) Konferencja Episkopatu Polski 13 marca 2018 r. wydała dekret ogólny w sprawie ochrony danych w Kościele katolickim. Dekret wszedł w życie z chwilą jego promulgacji, która nastąpiła 30 kwietnia 2018 r. przez zamieszczenie go na oficjalnej stronie internetowej Konferencji Episkopatu Polski. Biorąc pod uwagę zasady ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, stosowanych w Kościele katolickim w Polsce. Należy podkreślić że ochrona danych osobowych w Kościele była stosowana wiele lat przed wydaniem RODO. Regulowały ją Kodeks prawa kanonicznego z 1983 r. i Kodeks kanonów Kościołów Wschodnich z 1990 r. oraz przepisy Konferencji Episkopatu Polski w formie instrukcji lub dekretów ogólnych.

KS. DR HAB. JANUSZ BORUCKI (1962–). Polski prezbiter (1992) diecezji włocławskiej. Mgr: teologia, 1992 (KUL, Lublin); lic. nauk prawnych: prawo kanoniczne, 1996 (KUL, Lublin); dr nauk prawnych: prawo kanoniczne, 1998 (ATK, Warszawa); lic. nauk teologicznych: 2012 (UMK, Toruń); dr hab. nauk teologicznych: 2013 (UMK, Toruń). Pracownik (1998–), wiceoficjał (2001–2024) i oficjał (2024–) Sądu Kościelnego Diecezji Włocławskiej.

Nawiązując do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) oraz jego wejściem w życie (24 V 2016), Konferencja Episkopatu Polski (KEP) powołała zespół roboczy, by opracował wewnątrzkościelne regulacje dotyczące ochrony danych osobowych i dostosował obowiązujące regulacje do unijnych przepisów. Przygotowany został projekt aktu normatywnego jako dekret ogólny, który uchwalono podczas 377. Zebrania Plenarnego KEP dnia 13 października 2017 r. i przekazano do Stolicy Apostolskiej w celu uzyskania *recognitio*.

Dekret w ostatecznej formie (po wprowadzeniu zaleconych zmian) został uchwalony przez KEP 13 marca 2018 r. podczas 378. Zebrania Plenarnego KEP i ponownie przesłany do Stolicy Apostolskiej w celu uzyskania *recognitio*, które zostało udzielone 5 kwietnia 2018 r. Dekret wszedł w życie z chwilą jego promulgacji w dniu 30 kwietnia 2018 r. przez zamieszczenie go na oficjalnej stronie internetowej KEP[1].

1. Okoliczności powstania Dekretu

Przedstawiony wyżej Dekret ogólny KEP w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim z 2018 r. nie wskazuje wprost na bezpośrednią okoliczność jego powstania, czyli na treść art. 91 RODO. Nawet w preambule Dekretu nie znalazło się odwołanie do tego przepisu.

Przepis art. 91 RODO wyraźnie nakazuje dostosowanie przepisów kościelnych do regulacji europejskiej, stanowiąc w ust. 1: „Jeżeli w państwie członkowskim w momencie wejścia niniejszego rozporządzenia w życie kościoły i związki lub wspólnoty wyznaniowe stosują szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem danych, zasady takie mogą być nadal stosowane, pod warunkiem, że zostaną dostosowane do niniejszego rozporządzenia".

Konsekwencją zachowania pełnej autonomii Kościoła w tym przedmiocie jest też ust. 2 tegoż art. 91 RODO, nakazujący wprowadzenie w Kościołach lokalnych nadzoru niezależnych organów w tym przedmiocie (w Polsce jest nim Kościelny Inspektor Ochrony Danych – KIOD). Przepis

[1] P. Kroczek, P. Skonieczny, *Ochrona danych osobowych w Kościele katolickim. Komentarz do Dekretu ogólnego Episkopatu Polski w sprawie ochrony danych osobowych w Kościele katolickim z 2018 roku*, t. 1, cz. 1–2, Kraków 2022, s. 39–40, DOI: 10.15633/9788363241322.

ten stanowi: „Kościoły i związki wyznaniowe, które stosują szczegółowe zasady zgodnie z ust. 1 niniejszego artykułu, podlegają nadzorowi niezależnego organu nadzorczego, który może być organem odrębnym z zastrzeżeniem, że spełnia warunki określone w rozdziale VI niniejszego rozporządzenia".

Obecnie nie może być skutecznie podważane to, że Kościół katolicki w Polsce spełnił wszystkie przesłanki art. 91 RODO i tym samym mógł skorzystać z możliwości wyłączenia swojej działalności własnej (wewnętrznej) spod RODO. W tej dziedzinie Kościół cieszy się pełną autonomią – ma własne endogenne prawo, czyli w szczególności Dekret i swój organ nadzorczy, czyli KIOD. Taki był cel art. 91 RODO – zagwarantowanie związkom wyznaniowym autonomii w zakresie ochrony danych osobowych[2].

Kościół katolicki, podobnie jak inne związki wyznaniowe, ma prawo do gromadzenia, przetwarzania i przechowywania danych osobowych wszystkich tych, którzy są jego członkami. Dane te jednak powinny być traktowane w sposób respektujący prawo każdego człowieka do prywatności i ochrony gromadzonych na jego temat informacji. Należy podkreślić, że ochrona danych osobowych była standardem w Kościele katolickim wiele lat przed wejściem w życie RODO. Przed Dekretem ogólnym KEP w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych z 2018 r. w dniu 23 września 2009 r. została wydana Instrukcja kościelna pt. *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce*, opracowana przez Sekretariat KEP oraz Generalnego Inspektora Ochrony Danych Osobowych, która w zasadniczej części odwołuje się do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3].

Naczelny Sąd Administracyjny na posiedzeniu niejawnym 18 listopada 2022 r. rozpatrując skargę kasacyjną na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie w przedmiocie odmowy uaktualnienia danych osobowych, w uzasadnieniu wyroku wskazał, że w momencie wejścia w życie RODO tj. 24 maja 2016 r. w Kościele rzymskokatolickim istniała regulacja dotycząca przetwarzania danych osobowych, przede wszystkim w Kodeksie prawa kanonicznego, którą Kościół w terminie określonym w art. 91 ust. 1 RODO do 25 maja 2018 r. dostawał do przepisów wynikających z RODO[4].

---

[2] Tamże, s. 40–42.

[3] Zob. M. Czelny, *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce*, „Studia z Prawa Wyznaniowego", 14(2011), s. 241–168; J. Przybyłowski, *Ochrona danych osobowych w Kościele katolickim w Polsce*, StWł, 14(2012), s. 423–437.

[4] Zob. Naczelny Sąd Administracyjny, III OSK 2461/21 – Wyrok NSA, https://Orzeczenia.NSA.Gov.PL/doc/9441AC8CDD [7.08.2023].

2. Pojęcie „administrator danych osobowych”

Pojęcie „administrator danych osobowych” zostało zdefiniowane w art. 5 ust. 4 Dekretu ogólnego KEP z 2018 r.[5], nawiązując do Instrukcji z 2009 r. Zgodnie z brzmieniem tego przepisu administratorem danych osobowych jest osoba prawna lub inna jednostka organizacyjna, która ustala cele i sposoby przetwarzania danych osobowych. Są nimi: biskupi, proboszczowie oraz instytucje współpracujące z Kościołem, np. fundacje, stowarzyszenia. Należy więc domniemywać, że istnieje wiele innych organów reprezentujących Kościół katolicki, które mogą korzystać ze statusu „administratora danych osobowych”, a tym samym ze wszystkich praw i obowiązków z niego wynikających[6].

Powracając do pojęcia „administrator danych osobowych”, należy podkreślić, że wymienione warunki (dotyczące charakteru podmiotu oraz decydowania o celu i zakresie przetwarzania danych) muszą być spełnione łącznie. Ponadto podejmowanie decyzji o celu i zakresie przetwarzania danych musi być rzeczywiste (a więc nie pozorne) oraz samodzielne (dokonywane we własnym imieniu)[7]. Mówiąc o ochronie danych osobowych należy zauważyć, że w Dekrecie rozróżnia się pojęcia „dane osobowe”[8], „przetwarzanie”[9] oraz „zbiór danych”[10].

---

[5] Zob. Konferencja Episkopatu Polski, *Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim* (Dekret), https://episkopat.pl/promulgacja_dekretu_ogolnego_ws_ochrony_osob_fizycznych-2 [2.08.2023].

[6] Czelny, *Ochrona*, s. 243.

[7] Tamże; T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 14.

[8] Art. 5 ust. 1 Dekretu definiuje „dane osobowe” jako „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 indentyfikacyjny, dane lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”.

[9] Art. 5 ust. 2 Dekretu definiuje „przetwarzanie” jako „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowanie, adaptowanie lub modyfikowanie, pobierane, przeglądanie, wykorzystywanie, ujawnienia poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”.

[10] Art. 5 ust. 3 Dekretu definiuje „zbiór danych” jako „uporządkowany zestaw danych osobowych dostępnych według okresowych 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 rejestry ochrzczonych, bierzmowanych, Pierwszej Komunii Świętej, zawartych małżeństw,

3. Administrator danych osobowych a osoba upoważniona do ich przetwarzania

Przepisy prawa polskiego zawarte w ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych oraz Instrukcji kościelnej z 23 września 2009 r. *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce* stanowiły, że administrator danych osobowych nie musi sam przetwarzać danych. Powierzenie tej czynności innemu podmiotowi (zleceniobiorcy) nie prowadzi zatem do utraty statusu administratora danych, a co więcej – jest w pełni dopuszczalne. Zgodnie z przepisem art. 31 ust. 1 ustawy o ochronie danych osobowych, administrator danych mógł powierzyć innemu podmiotowi ich przetwarzanie w drodze umowy zawartej na piśmie. Ponadto podmiot, o którym mowa, mógł przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie[11]. Niedotrzymanie formy pisemnej umowy, jak również nieokreślenie w niej celu i zakresu formy przetwarzania danych, może skutkować powstaniem po stronie administratora odpowiedzialności za udostępnienie danych nieuprawnionemu podmiotowi lub jedynie utrudnieniami dowodowymi, zgodnie z art. 74 § 1 kodeksu cywilnego[12]. Po stronie zaś tego, komu powierzono przetwarzanie danych, niedotrzymanie formy pisemnej skutkuje odpowiedzialnością za niezgodne z prawem przetwarzanie danych w zbiorze. Podobny skutek powstaje w przypadku wykroczenia poza określony w umowie cel i zakres przetwarzania danych[13].

Obecnie obowiązujący Dekret z 2018 r. stanowi, że pojęcie „administrator" oznacza osobę prawną lub inną jednostkę organizacyjną, która ustala cele i sposoby przetwarzania danych osobowych (art. 5 ust. 4). Administrator nie musi osobiście przetwarzać danych, w jego imieniu może to robić „podmiot przetwarzający", którym może być osoba fizyczna lub prawna bądź jednostka organizacyjna (art. 5 ust. 5).

---

zgonów, jak również rejestr parafian, alumnów seminariów duchownych, nowicjuszy i członków instytutów życia konsekrowanego i stowarzyszeń życia apostolskiego".

[11] Szewc, *Publicznoprawna*, s. 16.

[12] „Zastrzeżenie formy pisemnej, dokumentowej albo elektronicznej bez rygoru nieważności ma ten skutek, że w razie niezachowania zastrzeżonej formy nie jest w sporze dopuszczalny dowód z zeznań świadków lub z przesłuchania stron na fakt dokonania czynności. Przepisu tego nie stosuje się, gdy zachowanie formy pisemnej, dokumentowej albo elektronicznej jest zastrzeżone jedynie dla wywołania określonych skutków czynności". Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. 1964, nr 16, poz. 93, z późn. zm.

[13] Czelny, *Ochrona*, s. 246.

4. Obowiązki administratora danych osobowych

Dekret ogólny KEP w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim z 2018 r. zawiera obowiązki administratora danych. Należy podkreślić, że takie obowiązki wyznaczają wcześniejsze przepisy obowiązujące zarówno w prawie polskim jak i w prawie kościelnym. Do podstawowych obowiązków administratora danych należą: obowiązki informacyjne (w stosunku do tych, których dotyczą przetwarzane dane), obowiązki rejestracyjne (co do zbiorów danych osobowych) oraz obowiązki zabezpieczenia danych (zwłaszcza ich poufności, integralności i nierozerwalności)[14].

4.1. Obowiązki informacyjne

Obowiązki informacyjne, obciążające administratora danych osobowych, wiążą się ściśle z uprawnieniami osób, których dane dotyczą (zainteresowanych). Jednym z najważniejszych jest więc obowiązek respektowania należnych im praw. Są to uprawnienia informacyjne, korekcyjne i zakazowe. W pierwszym przypadku chodzi wyłącznie o uzyskanie informacji od administratora danych różnego rodzaju. Informacje te mogą stanowić podstawę do wysuwania roszczeń korekcyjnych lub zakazowych. W uprawnieniach uwzględnionych w pozostałych grupach chodzi o możliwość podejmowania działań przez osobę, której dane dotyczą, a która zmierza do osiągnięcia reakcji administratora danych. Reakcja administratora polega odpowiednio na zmianie (rektyfikacji) danych lub zaprzestaniu ich przetwarzania[15].

W Dekrecie z 2018 r. rozdział III *Prawa osoby, której dane dotyczą* obejmuje art. 11–16. Zgodnie z art. 11 Dekretu 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 m.in. otrzymania szeregu informacji. Administrator ma także obowiązek wobec osoby, której dane dotyczą, dostarczyć bezpłatnie jej danych podlegających przetwarzaniu. Za wystawienie kolejnych kopii danych w postaci wyciągu, świadectwa lub dokumentu autentycznego można pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Poprzez słowo „kopia" należy rozumieć wszystkie informacje, które są przetwarzane przez administratora, a dotyczą osoby, która zgłasza

[14] Tamże, s. 248.

[15] Tamże, s. 249; Szewc, *Publicznoprawna*, s. 74.

żądanie, a nie dokładne odtworzenie oryginalnego dokumentu w wersji czy to elektronicznej (skan lub zdjęcie), czy to w postaci kserokopii.

W myśl art. 12 osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, jeżeli są nieprawidłowe. Wniosek taki powinien zostać przedstawiony w formie pisemnej administratorowi, osobiście lub za pośrednictwem prawnie ustanowionego pełnomocnika. Sprostowanie danych dotyczących aktów i faktów stanu kanonicznego osoby można dokonać jedynie za zezwoleniem ordynariusza miejsca lub wyższego przełożonego instytutu życia konsekrowanego lub stowarzyszenia życia apostolskiego. Jeżeli administrator odmówi przyjęcia wniosku, powinien pisemnie powiadomić wnioskodawcę.

Osoba, której dane dotyczą, ma prawo w uzasadnionym zakresie żądać umieszczenia w zbiorze danych adnotacji lub uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowych oświadczeń. Adnotacja dokonana na marginesie dokumentów stanowi jego część integralną. Jej treść powinna być umieszczana w każdym wyciągu lub kopii akt (art. 13).

Prawo do żądania usunięcia danych, czyli tak zwane „prawo do zapomnienia" nie miało na gruncie poprzedniego stanu prawnego i nie będzie miało także po wejściu w życie RODO pełnego zastosowania do działalności wewnętrznej, czyli statutowej Kościoła. Prawo to, zgodnie z regulacjami zawartymi w RODO w stosunku do Kościoła i innych związków wyznaniowych, zostało wyłączone przez Dekret. Oczywiście, prawo do żądania usunięcia danych przysługuje, lecz nie w przypadku, gdy dane dotyczą udzielonych sakramentów bądź w inny sposób odnosi się do kanonicznego statusu osoby, np. przyjętej profesji zakonnej. Ograniczenie „prawa do zapomnienia" wynika z racji teologicznej, np. z niezniszczalnego charakteru chrztu świętego (kan. 849 KPK) prawa bezwzględnie stosowanego w Kościele. Takie rozwiązanie prawne szanujące niezależność i autonomię Kościoła w sprawach religijnych jest zgodne z prawem polskim np. art. 25 ust. 3 Konstytucji RP z 2 kwietnia 1997 r. czy art. 1 Konkordatu z 28 lipca 1993 r. oraz prawem unijnym np. Traktatem o funkcjonowaniu Unii Europejskiej. Tego typu żądanie usunięcia danych, mimo jego niedopuszczalności na mocy art. 14 ust. 4 Dekretu, powinno zostać odnotowane w zbiorze (np. księdze chrztów). Osoba, której dane dotyczą, może żądać od administratora niezwłocznego usunięcia danych osobowych, 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, cofnie zgodę, na której opiera się przetwarzanie danych i nie ma innej podstawy prawnej przetwarzania; 3) dane osobowe były przetwarzane niezgodnie z prawem. W takich przypadkach administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe (art. 14 ust. 1).

Dekret precyzuje też prawo do żądania ograniczenia przetwarzania danych. Ma ono zastosowanie w przypadku, 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 (art. 15).

Administrator danych ma obowiązek powiadomienia osoby, której dane dotyczą, o odbiorcach, którym ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub czynność ta będzie wymagać niewspółmiernie dużego wysiłku (art. 16).

4.2. Obowiązek zabezpieczenia danych

Obowiązki administratora związane z zabezpieczeniem danych osobowych[16] szczegółowo określono w prawie polskim jeszcze przed wejściem w życie RODO. Regulacji takiej dokonano w przepisach rozdziału piątego ustawy o ochronie danych z dnia 29 sierpnia 1997 r. oraz w rozporządzeniu wykonawczym do tej ustawy wydanym przez Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004, nr 100, poz. 1024)[17].

Obowiązki administratora związane z zabezpieczaniem danych wiążą się ściśle z realizacją zasady poufności. Obowiązki te odnoszą się do

[16] Pod pojęciem „zabezpieczenie danych" rozumie się wszystkie przedsięwzięcia o charakterze technicznym i organizacyjnym podejmowane w celu zabezpieczenia zgromadzonych danych przed zniszczeniem lub uszkodzeniem, jak również przed wszelkiego rodzaju nadużyciami. Zob. A. Mrózek, *Ustawowe prawo ochrony danych – analiza prawno-porównawcza*, Toruń 1981, s. 25

[17] Czelny, *Ochrona*, s. 258.

organizacyjnych i technicznych aspektów przetwarzania danych i nakazują zachowanie ich w tajemnicy wobec osób, które nie są uprawnione do dostępu do nich oraz podjęcie stosownych środków pozwalających na skuteczną ich ochronę. Zasada poufności i zabezpieczania danych opiera się na założeniu, że dla skutecznej ochrony danych osobowych konieczne jest zapewnienie należytego zabezpieczenia przetwarzanych danych. Wszystkie mechanizmy zabezpieczania danych powinny być proporcjonalne do zagrożeń i kategorii przetwarzania danych[18].

Do obowiązków związanych z zabezpieczeniem danych osobowych przez administratora nawiązuje Instrukcja kościelna z 2009 r. Instrukcja stanowi, że administrator ma obowiązek zabezpieczyć dane osobowe poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych, tak aby: nie były one udostępnione osobom nieupoważnionym, nie były zabrane przez osobę nieupoważnioną oraz były zabezpieczone przed uszkodzeniem, zniszczeniem lub utratą. Do innych obowiązków administratora dotyczących prawidłowego zabezpieczenia danych osobowych zalicza się także obowiązek dołożenia szczególnej staranności przy przetwarzaniu i należytym ich zabezpieczaniu. Obowiązek ten ma na celu ochronę interesów osób, których dane dotyczą[19].

Dekret ogólny Konferencji Episkopatu Polski z 2018 r. w rozdziale IV, art. 17 stanowi, że administrator danych powinien: 1) wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia prawa lub wolności osób fizycznych; 2) wdrożenie odpowiedniej polityki ochrony danych; 3) na etapie projektowania, jak też w trakcie procesów przetwarzania 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[20].

4.3. Obowiązki wynikające z unormowań kościelnych

Instrukcja kościelna z 2009 r. w części II ust. 6 podaje obowiązki administratora danych wynikające z Kodeksu prawa kanonicznego

[18] Zob. P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008, s. 48.

[19] Czelny, *Ochrona*, s. 259.

[20] Zob. Dekret, rozdział IV, art. 17 dekret ogólny.

z 1983 r.[21] Powołując się na kan. 486–491 KPK, w Instrukcji określono zasady dotyczące archiwizacji dokumentów, tym samym regulując kwestię zabezpieczenia danych osobowych w Kościele katolickim[22].

Dekret z 2018 r. rozdział IV poświęca obowiązkom administratora danych i podmiotu przetwarzającego art. 17–34.

Administrator danych został zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia prawa osób fizycznych. Już na etapie projektowania a następnie przetwarzania danych administrator powinien zastosować odpowiednie środki techniczne i organizacyjne pozwalające bezpiecznie przetwarzać dane. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i przetwarzanie danych, to razem określają zakres swoich obowiązków i odpowiedzialności (art. 17–18).

Jeżeli przetwarzanie ma być dokonane w imieniu administratora przez podmiot przetwarzający, podmiot ten powinien zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie gwarantowało ochronę praw osób, których dane dotyczą. Przetwarzanie danych przez podmiot przetwarzający powinno opierać się na umowie zawartej z administratorem danych lub innym zobowiązaniu prawnym ustalającym zakres odpowiedzialności i zachowanie odpowiedniej procedury przetwarzania danych. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez pisemnej zgody administratora. Administrator danych oraz inna osoba posiadająca stały dostęp do danych gromadzonych lub nabytych ma obowiązek zachowania tajemnicy dotyczącej wszystkich przetwarzanych danych osobowych. Obowiązek ten pozostaje także po zakończeniu pełnienia funkcji (art. 19–20).

Każdy administrator powinien prowadzić rejestr czynności przetwarzania danych osobowych, za które odpowiada, również podmiot przetwarzający powinien prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa przetwarzania danych. Podejmują również działania, by każda osoba fizyczna, która ma

[21] Szerzej zob. A. Mezglewski, *Działalność związków wyznaniowych a ochrona danych osobowych*, „Studia z Prawa Wyznaniowego", 10(2007), s. 17–18, DOI: 10.31743/spw.271.

[22] Czelny, *Ochrona*, s. 260–261.

dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo (art. 21–22).

Dekret z 2018 r. określa warunki, jakie powinien spełnić administrator przechowujący i przetwarzający dane osobowe. Zbiory danych powinny być przechowywane w pomieszczeniu przeznaczonym do tego celu, odpowiednio zabezpieczonym, do którego dostęp ma wyłącznie administrator, podmiot przetwarzający oraz osoby przetwarzające dane na podstawie upoważnienia. W przypadku braku oddzielnego pomieszczenia dane przechowuje się w specjalnych szafach gwarantujących ich bezpieczeństwo. Szczególną uwagę administrator danych powinien zwrócić na zabezpieczenie archiwum i jego zarządzanie. Archiwum powinno być wyposażone w system zamknięcia, który gwarantuje wystarczającą ochronę przed kradzieżą i włamaniem. Klucze do archiwum powinny być starannie przechowywane. Administrator powinien dochować staranności, udzielając dostępu do archiwum osobom postronnym. Dane osobowe przechowywane w archiwach cyfrowych powinny być zarządzane za pomocą licencjonowanego oprogramowania. Urządzenia i nośniki zawierające dane powinny być przechowywane w pomieszczeniach zamkniętych i zabezpieczonych. Tajne archiwum, ustanowione na podstawie ogólnych przepisów kanonicznych powinno być strzeżone, zgodnie z przepisami kan. 489–490 Kodeksu prawa kanonicznego[23] oraz kan. 259–260 Kodeksu kanonów Kościołów Wschodnich (art. 23–26).

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż 72 godziny po stwierdzeniu naruszenia – zgłasza je Kościelnemu Inspektorowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia prawa lub wolności osób fizycznych. Podmiot przetwarzający bez zbędnej zwłoki zgłasza je administratorowi. Jeżeli naruszenie danych osobowych może powodować wysokie naruszenie praw lub wolności osób fizycznych, administrator bez zwłoki zawiadamia

[23] KPK, kan. 489, § 1: „W kurii diecezjalnej powinno także być archiwum tajne albo przynajmniej w ogólnym archiwum powinna się znajdować kasa pancerna, dobrze zamknięta i umocowana, której nie da się wynieść z miejsca; należy tam przechowywać z największą starannością dokumenty tajne", § 2: „Każdego roku należy zniszczyć dokumenty spraw karnych dotyczących obyczajów, gdy oskarżone w nich osoby zmarły, albo spraw zakończonych przed dziesięciu laty wyrokiem skazującym, zachowując krótkie streszczenie faktu wraz z tekstem wyroku kończącego postępowanie". Kan. 490, § 1: „Klucz do tajnego archiwum może mieć tylko biskup", § 2: „Podczas wakansu stolicy nie wolno otwierać tajnego archiwum lub kasy pancernej, chyba że w razie prawdziwej konieczności uczyni to osobiście administrator diecezjalny", § 3: „Z tajnego archiwum lub kasy pancernej nie wolno wynosić dokumentów".

osobę, której dane zostały naruszone. Administrator powinien również zgłaszać bezzwłocznie właściwej władzy kościelnej, a w razie potrzeby także organom ścigania, każde wtargnięcie do archiwum lub do pomieszczenia, w których przechowywane są zbiory danych, którego skutkiem była utrata lub zniszczenie rejestrów, akt, dokumentów, indeksów i katalogów zawierających dane osobowe (art. 27–29).

W celu zapewnienia właściwej ochrony, gdy przetwarzanie danych odbywa się na dużą skalę, kościelna publiczna osoba prawna powinna wyznaczyć inspektora ochrony danych (art. 30).

5. Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

Ważne miejsce wśród unormowań określających pozycję prawną administratora danych osobowych zajmują regulacje odnoszące się do jego odpowiedzialności za naruszenie przepisów o ochronie danych osobowych. Gdy chodzi o odpowiedzialność administratora, mamy dwie możliwości.

Dekret ogólny Konferencji Episkopatu Polski z 13 marca 2018 r. o ochronie danych osobowych i tylko Dekret stosuje się do publicznych kościelnych osób prawnych (czyli np. parafii, diecezji, publicznych stowarzyszeń wiernych) w zakresie wykonywania przez nie działalności wewnętrznej, czyli działalności w zakresie swoich spraw. Są to więc wyłącznie sprawy związane z misją Kościoła i są wykonywaniem jego wewnętrznych zadań objętych co do zasady prawem kanonicznym.

Z kolei w sprawach mieszanych (kościelno-państwowych) określanych jako *causa mixtae* (*res mixtae*), czyli tych, które leżą w kompetencji i Kościoła, i państwa, stosuje się do ochrony danych osobowych również oprócz Dekretu, także RODO i ustawę o ochronie danych osobowych[24] oraz inne ustawy. Państwo bowiem jest zainteresowane regulacją tych sfer życia i reguluje je poprzez różne akt normatywne. Do takich spraw zalicza się przykładowo: posiadanie cmentarzy, sprawy majątkowe i podatkowe, pomoc społeczną, ochronę dóbr kultury i dziedzictwa narodowego.

* * *

Chrześcijaństwo wniosło do kultury europejskiej przekonanie o nienaruszalności godności osoby ludzkiej. Zakorzenione ono jest w fakcie stworzenia człowieka na „obraz i podobieństwa" Boga. Godność jest

[24] Zob. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018, poz. 1000.

przymiotem ludzkiej natury rozumnej i wolnej. Uznanie godności człowieka wymaga odpowiedniej ochrony danych osobowych[25].

Biorąc pod uwagę zasady ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, stosowanych dotychczas w Kościele katolickim w Polsce, w porządku chronologicznym, należy uwzględnić:

1) przepisy Konferencji Episkopatu Polski o prowadzeniu ksiąg parafialnych: ochrzczonych, bierzmowanych, małżeństw i zmarłych, oraz księgi stanu dusz z dnia 26 października 1947 r.;
2) kan. 220 Kodeksu prawa kanonicznego z 1983 r. oraz kan. 23 Kodeksu kanonów Kościołów Wschodnich z 1990 r., gwarantujące prawo do dobrego imienia i prawo do ochrony intymności;
3) kan. 482–491, 535 Kodeksu prawa kanonicznego oraz kan. 252–261, 296 Kodeksu kanonów Kościołów Wschodnich, zobowiązujące każdą parafię do prowadzenia ksiąg parafialnych oraz zobowiązujące proboszcza do ich właściwego sporządzania i przechowywania oraz dotyczące obowiązku posiadania archiwum przez kurie diecezjalne i parafie;
4) kan. 1067 i 1069 Kodeksu prawa kanonicznego oraz kan. 784 i 786 Kodeksu kanonów Kościołów Wschodnich, dotyczące przygotowania do małżeństwa;
5) Instrukcję opracowaną przez Generalnego Inspektora Ochrony Danych Osobowych oraz Sekretariat Konferencji Episkopatu Polski z dnia 23 września 2009 r. dotyczącą ochrony danych osobowych w działalności Kościoła katolickiego w Polsce;
6) Dekret ogólny Konferencji Episkopatu Polski w sprawie wystąpień z Kościoła oraz powrotu do wspólnoty Kościoła z dnia 7 października 2015 r.;
7) Dekret ogólny Konferencji Episkopatu Polski w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim z dnia 13 marca 2018 r.

PROTECTION OF PERSONAL DATA AND THEIR PROCESSING IN THE CATHOLIC CHURCH IN POLAND

Keywords: personal data protection, general decrees of the Polish Episcopal Conference, Code of Canon Law.

Abstract: After the entry into force of the Regulation of the European Parliament and of the Council (EU) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

[25] Kroczek, Skonieczny, *Ochrona*, s. 7.

free movement of such data (GDPR), the Polish Episcopal Conference on March 13 in 2018 issued a general decree on data protection in the Catholic Church. The decree entered into force upon its promulgation, which took place on April 30, 2018, by posting it on the official website of the Polish Episcopal Conference. Taking into account the principles of protection of natural persons in connection with the processing of their personal data applied in the Catholic Church in Poland, it should be emphasized that such protection was applied many years before the issuance of the GDPR. Data protection in the Church was and still is regulated by the canons of the Code of Canon Law of 1983 and the Code of Canons of the Eastern Churches of 1990, as well as regulations issued by the Polish Episcopal Conference in the form of instructions or general decrees.

BIBLIOGRAFIA

Codex Iuris Canonici. Kodeks prawa kanonicznego. Stan prawny na dzień 18 maja 2022 roku. Zaktualizowany przekład na język polski, Poznań 2022.

Konferencja Episkopatu Polski, *Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim*, https://episkopat.pl/promulgacja_dekretu_ogolnego_ws_ochrony_osob_fizycznych-2 [2.08.2023].

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz. U. 1964, nr 16, poz. 93, z późn. zm.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018, poz. 1000.

Naczelny Sąd Administracyjny, III OSK 2461/21 – Wyrok NSA, https://Orzeczenia.NSA.Gov.PL/doc/9441AC8CDD [7.08.2023]

Czelny M., *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce*, „Studia z Prawa Wyznaniowego", 14(2011), s. 241–268.

Fajgielski P., *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008.

Kroczek P., Skonieczny P., *Ochrona danych osobowych w Kościele katolickim. Komentarz do Dekretu ogólnego Episkopatu Polski w sprawie ochrony danych osobowych w Kościele katolickim z 2018 roku*, t. 1, cz. 1–2, Kraków 2022, DOI: 10.15633/9788363241322.

Mezglewski A., *Działalność związków wyznaniowych a ochrona danych osobowych*, „Studia z Prawa Wyznaniowego", 10(2007), s. 5–21, DOI: 10.31743/spw.271.

Mrózek A., *Ustawowe prawo ochrony danych – analiza prawno-porównawcza*, Toruń 1981.

Przybyłowski J., *Ochrona danych osobowych w Kościele katolickim w Polsce*, StWł, 14(2012), s. 423–437.

Szewc T., *Publicznoprawna ochrona informacji*, Warszawa 2007.