STUDIA Z PRAWA WYZNANIOWEGO
Tom 14 – 2011

MICHAŁ CZELNY

# OCHRONA DANYCH OSOBOWYCH W DZIAŁALNOŚCI KOŚCIOŁA KATOLICKIEGO W POLSCE

Rozwój naszej cywilizacji jest bardzo ściśle związany z rozwojem informacji. Wiek XX zakończył się prawdziwą eksplozją nowych możliwości gromadzenia danych i ich przetwarzania w sposób elektroniczny. Informacja stała się cennym towarem, który jest chroniony nie tylko w porządkach prawnych poszczególnych państw oraz w prawie międzynarodowym i unijnym, ale również na gruncie unormowań kościelnych. Kościelne uregulowania dotyczące ochrony danych osobowych stanowią jednak w Polsce swego rodzaju nowum, a związane z tym kwestie praktyczne wywołują wiele pytań i kontrowersji.

Trudno mieć wątpliwości, że Kościół katolicki, podobnie jak inne związki wyznaniowe, ma prawo do gromadzenia 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. Zadanie odpowiedniej ochrony danych osobowych oraz poszanowania zasad ich przetwarzania spoczywa więc również na jednostkach organizacyjnych Kościoła katolickiego.

Niniejsze opracowanie opiera się przede wszystkim na analizie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] oraz instrukcji kościelnej z dnia 23 września 2009 r. *Ochrona danych osobo-*

[1] Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm. Dalej: OchrDanU.

*wych w działalności Kościoła katolickiego w Polsce*[2]*,* która w zasadniczej części odwołuje się do wspomnianego wyżej aktu normatywnego.

## 1. POJĘCIE „ADMINISTRATORA DANYCH OSOBOWYCH"

Pojęcie „administratora danych osobowych" zostało zdefiniowane w art. 7 pkt 4 ustawy o ochronie danych osobowych. Zgodnie z brzmieniem tego przepisu administratorem danych osobowych jest podmiot decydujący o celach i środkach przetwarzania danych osobowych. Może to być organ państwowy, organ samorządu terytorialnego, państwowa i komunalna jednostka organizacyjna, podmiot niepubliczny realizujący zadania publiczne, a także osoba fizyczna i osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną przetwarzająca dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Wszystkie wyżej wymienione podmioty winny mieć swoją siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Dyrektywa Parlamentu Europejskiego i Rady z 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (95/46/WE)[3] w art. 2 lit. d także definiuje pojęcie „administratora danych osobowych". Za „administratora danych" uznano w dyrektywie osobę fizyczną lub

[2] Konferencja Episkopatu Polski, *Ochrona danych osobowych w działalności Kościoła katolickiego w Polsce. Instrukcja opracowana przez Generalnego Inspektora Ochrony Danych Osobowych oraz Sekretariat Konferencji Episkopatu Polski,* z dnia 23 września 2009 r., „Akta Konferencji Episkopatu Polski" 2009, t. 2 (16), s. 53-59. Dalej: Instrukcja kościelna. Do Instrukcji kościelnej dołączono odpowiedzi Generalnego Inspektora Danych Osobowych na postawione mu pytania związane z działalnością Kościoła katolickiego w Polsce. W dalszej części niniejszego opracowania autor będzie się do nich odwoływał, wskazując jedynie na numer pytania.

[3] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Nr 95/46/WE) - Dz. Urz. UE L 281, z dnia 23 listopada 1995 r., s. 0031 i n.

prawną, urząd publiczny, agendę lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. Jeżeli cele i sposoby przetwarzania danych są określone w ustawach i innych przepisach krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalone przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty.

Do przytoczonej wyżej definicji ustawowej odnosi się także Instrukcja kościelna z 2009 r. W części II ust. 2 Instrukcji wskazano, że administratorem danych osobowych jest podmiot decydujący o celach i środkach przetwarzania danych osobowych, a więc Kościół katolicki reprezentowany przez właściwe organy, np. biskupów czy proboszczów oraz instytucje współpracujące z Kościołem (np. fundacje, stowarzyszenia, wydawnictwa)[4]. Możemy zauważyć, że powoływana w tym miejscu Instrukcja kościelna wymienia jedynie przykładowe organy reprezentujące Kościół katolicki jako podmiot określany mianem „administratora danych osobowych". Są nimi: biskupi, proboszczowie oraz instytucje współpracujące z Kościołem, które też są wymienione jedynie przykładowo (fundacje, stowarzyszenia czy wydawnictwa). Należy więc domniemywać, że istnieje wiele innych organów reprezentujących Kościół katolicki jako „administratora danych osobowych", które nie są w tym miejscu uwzględnione, a które mogą także korzystać ze statusu „administratora danych osobowych", a tym samym ze wszelkich praw i obowiązków z niego wynikających.

Powracając do ustawowej definicji „administratora danych osobowych", należy podkreślić, że wymienione warunki (dotyczące charakteru podmiotu oraz decydowania o celu i zakresie przetwarzania danych) muszą być spełnione łącznie[5]. Ponadto podejmowanie decyzji o celu i zakresie przetwarzania danych musi być rzeczywiste (a więc nie pozorne) oraz samodzielne (dokonywane we własnym imieniu)[6].

---

[4] Zob. część II ust. 2 (*initio*) Instrukcji kościelnej.

[5] Zob. T. Szewc, *Publicznoprawna ochrona informacji,* Warszawa 2007, s. 14.

[6] Zob. A Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism, przepisy,* wyd. 3, Warszawa 2007, s. 66-69; T. Szewc, *Publicznoprawna ochrona,* s. 15. Decydowanie o celu i zakresie przetwarzania danych może być wynikiem świadomego wyboru (np. w następstwie podjęcia określonej działalności, z którą łączy się decydowanie o przetwarza-

Istotną trudność stanowi wskazanie podmiotu publicznego, który posiada status administratora danych, a który to podmiot został przykładowo wymieniony w Instrukcji kościelnej z 2009 r. Trudność ta wynika: po pierwsze – z braku określenia szczegółowych kompetencji do działania przez podmioty publiczne o celu i środkach przetwarzania danych oraz – po drugie – z wielości podmiotów publicznych, obejmującego organy państwowe i samorządowe jednostki organizacyjne, pomiędzy którymi może ponadto występować przekazywanie zadań[7].

Ponadto administratorem danych nigdy nie jest określona osoba pełniąca funkcję w imieniu jednostki przetwarzającej dane osobowe, bo w przytoczonej wyżej ustawowej definicji „administratora danych" rysuje się organizacyjna a nie personalna koncepcja administratora[8]. Należy też zauważyć, że w ustawie o ochronie danych osobowych rozróżnia się pojęcia: „administrator danych", „administrujący zbiorem danych"[9] oraz „administrujący danymi osobowymi"[10].

---

niu danych osobowych), jak również następstwem obowiązku decydowania o przetwarzaniu danych. Decyzja o przetwarzaniu danych pozostaje w gestii jednego podmiotu. Jeżeli decydowanie o celu i środkach przetwarzania danych zostało pozostawione różnym podmiotom (przykładowo podmiot A decyduje o celu zbierania danych, a podmiot B o środkach ich opracowywania i utrwalania), żaden z nich nie ma wówczas statusu administratora danych osobowych (zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* wyd. 4, Kraków 2007, s. 379). Jednak ustawa o ochronie danych osobowych nie stoi na przeszkodzie współadministrowania danymi (np. przez przedsiębiorców realizujących wspólne przedsięwzięcie). Administratorzy wspólnie rozstrzygają wówczas o celach przetwarzanych i o środkach przetwarzanych danych. Typowym przykładem takich administratorów mogą być wspólnicy spółki cywilnej. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 15.

[7] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 14. Problematyka podmiotów publicznych przyporządkowywanych do definicji „administratora danych osobowych" jest uwzględniona przez Instrukcję kościelną z 2009 r. a zadania i kompetencje administratora danych wykonują jego przykładowo wymienione w niej organy.

[8] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 377-378; T. Szewc, *Publicznoprawna ochrona,* s. 15.

[9] Zob. Art. 51 ust. 1 OchrDanU. Art. 7 pkt 1 OchrDanU definiuje „zbiór danych osobowych" jako „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie". Identyczną definicje podaje Instrukcja kościelna w części I ust. 3. Z definicji ustawowej wynika, że zbiór informacji uzyskuje status zbioru danych osobowych, jeżeli spełnione są następujące warunki:

– w skład zbioru musi wchodzić zestaw danych o charakterze osobowym, wobec tego nie tworzą go pojedyncze informacje o osobie, lecz dopiero informacje powiązane ze sobą

## 2. ADMINISTRATOR DANYCH OSOBOWYCH A OSOBA UPOWAŻNIONA DO ICH PRZETWARZANIA

Administrator danych osobowych nie musi sam przetwarzać danych. Powierzenie tej czynności innemu podmiotowi (zleceniobiorca) nie prowadzi zatem do utraty statusu administratora danych, a co więcej – jest w pełni dopuszczalne[11]. Jest to zgodne w szczególności z art. 31 ust. 1 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem „administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych". Ponadto podmiot, o którym mowa, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie[12]. Niedotrzymanie formy pisemnej umowy, jak również nieokreślenie w niej celu i zakresu przetwarzania danych, może skutkować powstaniem po stronie administratora odpowiedzialności za udostępnianie danych nieuprawnionemu podmiotowi (lub idąc za J. Bartą, P. Fajgielskim

---

i umożliwiające określenie tożsamości osoby, której dotyczą. Stąd muszą to być co najmniej dane identyfikujące;

– zbiór musi posiadać strukturę – dane w tym zbiorze muszą być uporządkowane. Struktura pozwala na odnalezienie danych bez potrzeby przeglądania wszystkich informacji zawartych w zestawie;

– w zbiorze dane dostępne są według określonych kryteriów – dostępność zbioru danych oznacza, że taki zbiór musi być umieszczony na wystarczająco trwałym nośniku. Oprócz tego zbiór danych musi też umożliwiać odnalezienie danych osobowych według określonych kryteriów. Generalny Inspektor Ochrony Danych Osobowych opowiedział się za stanowiskiem, że zbiorem danych jest struktura, która umożliwia dostęp do danych według kryterium przyjętego przez administratora za wystarczające, stąd OchrDanU używa określenia „kryteria" w liczbie mnogiej dla podkreślenia ich wielorakości. Jeżeli kryterium jest jedno, to zbiór taki będzie jedynie zbiorem ewidencyjnym, a jeżeli kryteriów jest więcej niż jedno, to zbiór będzie nosił miano zbioru danych. Istnieją jednak odmienne stanowiska, według których zbiór ewidencyjny jest odmianą zbioru danych, z tym że umożliwiającym dostęp wyłącznie według jednego kryterium. Rozwiązanie tej kwestii nie stanowi jednak przedmiotu niniejszego artykułu. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 11-13; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 363; A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 1999, s. 27; Generalny Inspektor Ochrony Danych Osobowych, Pytania dotyczące definicji zbiorów danych osobowych, http://www.giodo.gov.pl/320/id_art./1475/j/pl/ - dostęp 18.12.2010 r.

[10] Zob. Art. 52 OchrDanU.

[11] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 16.

[12] Zob. Art. 31 ust. 2 OchrDanU.

i R. Markiewiczem, jedynie utrudnieniami dowodowymi, zgodne z art. 74 § 1 KC[13]). Po stronie zaś tego, komu powierzono przetwarzanie danych, niedotrzymanie formy pisemnej skutkuje odpowiedzialnością za niezgodne z prawem przetwarzanie danych w zbiorze[14]. Podobny skutek powstanie w przypadku wykroczenia poza określony w umowie cel i zakres przetwarzania danych[15].

Obowiązkiem administratora danych jest dopuszczenie do przetwarzania danych osobowych osób, które wcześniej do tego przetwarzania upoważnił, zgodnie z art. 37 ustawy o ochronie danych osobowych[16]. Chodzi tu w szczególności o pracowników administratora. Osoby te wykonują prawa i obowiązki administratora w zakresie przetwarzania danych osobowych. Ustawa nie stawia takim osobom żadnych dodatkowych wymagań. Upoważnienie winno być jednak indywidualne (imienne), wyraźne i odrębne od stosunku prawnego łączącego administratora z osobą upoważnioną. Jeżeli dana osoba jest upoważniona tylko do niektórych czynności lub do przetwarzania tylko niektórych kategorii danych osobowych, to powinno to znaleźć odzwierciedlenie w treści upoważnienia[17].

---

[13] Ustawa z dnia 18 maja 1964 r. – Kodeks cywilny, Dz. U. Nr 16, poz. 93, z późn. zm. Art. 74 § 1 KC stanowi: „zastrzeżenie formy pisemnej bez rygoru nieważności ma ten skutek, że w razie niezachowania zastrzeżonej formy nie jest w sporze dopuszczalny dowód ze świadków ani dowód z przesłuchania stron na fakt dokonania czynności. Przepisu tego nie stosuje się, gdy zachowanie formy pisemnej jest zastrzeżone jedynie dla wywołania określonych skutków czynności prawnej". Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 562-563; T. Szewc, *Publicznoprawna ochrona,* s. 16.

[14] Zob. Art. 49 OchrDanU; T. Szewc, *Publicznoprawna ochrona*, s. 16.

[15] Przez cel przetwarzania danych należy tu rozumieć rezultat, jaki ma osiągnąć zleceniobiorca w następstwie przetwarzania danych, natomiast określenie zakresu obejmuje nie tylko rodzaj danych, lecz także rodzaj czynności, jakie osoba trzecia może na danych wykonywać. Dla przykładu możemy tutaj za T. Szewcem podać, że celem wskazanym w umowie może być przeprowadzenie kampanii reklamowej, zakresem czynności zaś zebranie danych klientów, a zakresem danych – imię, nazwisko, miejsce zamieszkania klienta. Szerzej na temat pozycji prawnej zleceniobiorcy: T. Szewc, *Publicznoprawna ochrona,* s. 16-17.

[16] Art. 37 OchrDanU stanowi, że „do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych".

[17] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 613-615; T. Szewc, *Publicznoprawna ochrona,* s. 18, 68.

Powyżej analizowana kwestia nie została uwzględniona w Instrukcji kościelnej z 2009 r., stąd przy dopuszczaniu do przetwarzania danych osobowych osób upoważnionych przez administratora danych osobowych w jednostkach organizacyjnych Kościoła katolickiego należy się kierować unormowaniami zawartymi w ustawie o ochronie danych osobowych.

Szczególnym przypadkiem osoby upoważnionej do przetwarzania danych osobowych jest administrator bezpieczeństwa informacji. Zadaniem administratora bezpieczeństwa informacji jest nadzorowanie przestrzegania zasad ochrony (tj. stosowania środków technicznych i organizacyjnych ochrony danych osobowych), chyba że podmiot przetwarzający dane sam wykonuje te czynności. W praktyce oznacza to konieczność powołania administratora bezpieczeństwa informacji przez wszystkie podmioty niebędące osobami fizycznymi, ponieważ nie są one w stanie same wykonywać wspomnianych wyżej czynności. Wobec powyższego możemy powiedzieć, że płaszczyzna działania administratora bezpieczeństwa informacji koncentruje się na zabezpieczaniu danych osobowych[18].

Administrator bezpieczeństwa informacji może być wyłącznie osobą fizyczną. Wynika to z art. 36 ust. 3 ustawy o ochronie danych osobowych, który stanowi, że administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony związanych z zabezpieczeniem danych osobowych, chyba że sam wykonuje te czynności[19]. Ponadto osoba pełniąca funkcję administratora bezpieczeństwa informacji powinna posiadać odpowiednią wiedzę z zakresu informatyki oraz znajomość przepisów dotyczących

[18] Powołanie administratora bezpieczeństwa informacji jest niezależne od sposobu przetwarzania danych osobowych – ręcznego bądź w systemie informatycznym. Rodzaj stosunku prawnego łączącego administratora bezpieczeństwa informacji z administratorem danych jest obojętny. Pozycję administratora bezpieczeństwa informacji w strukturach administratora danych powinna cechować niezależność od pionu informatycznego. Wynika to z faktu, że omawiany tu administrator go kontroluje. Możliwe jest połączenie funkcji administratora bezpieczeństwa informacji z pełnomocnikiem ochrony, podlegającego bezpośrednio kierownikowi jednostki organizacyjnej. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 18, 67; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 608-609; A. Drozd, *Ustawa o ochronie danych,* s. 263-265.

[19] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 68.

ochrony danych osobowych (tzn. posiadanie odpowiednich kwalifikacji i wiedzy)[20].

Instrukcja kościelna z 2009 r. w żadnym miejscu nie wskazuje na możliwość wyznaczenia osoby administratora bezpieczeństwa informacji, która by nadzorowała przestrzeganie zasad ochrony danych osobowych. Administrator danych osobowych, dając upoważnienie administratorowi bezpieczeństwa informacji, mógłby tym samym zwiększyć poczucie bezpieczeństwa związane z ochroną danych osobowych przetwarzanych przez jednostki organizacyjne Kościoła katolickiego w Polsce.

## 3. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

Wskazuje się, że do podstawowych obowiązków administratora danych osobowych należą: obowiązki informacyjne (w stosunku do tych, których dotyczą przetwarzane dane), obowiązki rejestracyjne (co do zbiorów danych osobowych) oraz obowiązki zabezpieczania danych (zachowania ich poufności, integralności i nienaruszalności). Wspomniane wyżej obowiązki administratora danych dzieli się ponadto ze względu na ich charakter na: obowiązki administracyjne, osobowe i techniczne[21].

### 3.1.OBOWIĄZKI INFORMACYJNE

Obowiązki informacyjne, obciążające administratora danych osobowych, wiążą się ściśle z uprawnieniami osób, których dane dotyczą (zainteresowanych). Jednym z najważniejszych jest więc obowiązek

[20] Zob. P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne,* Lublin 2008, s. 189. Szerzej na temat administratora bezpieczeństwa informacji: A. Bierć, *Sytuacja prawna administratora bezpieczeństwa informacji jako podmiotu zobowiązanego do kontroli stanu ochrony danych osobowych w przedsiębiorstwie,* „Przegląd Legislacyjny" 2000, nr 4; P. Fajgielski, *Kontrola przetwarzania,* s. 188-197.

[21] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych,* s. 378-379.

respektowania należnych im praw[22]. W zakresie właściwego zabezpieczania danych osobowych, na podstawie w art. 32 ust. 1 ustawy o ochronie danych osobowych, wyróżnia się trzy grupy uprawnień osób, których dane dotyczą. Są to uprawnienia informacyjne, korekcyjne i zakazowe[23]. 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 określonej reakcji administratora danych. Reakcja administratora polega odpowiednio na zmianie (rektyfikacji) danych lub zaprzestaniu ich przetwarzania[24]. Uprawnień informacyjnych nie należy mylić z obowiązkiem informacyjnym, uregulowanym w art. 24 i 25 ustawy o ochronie danych osobowych[25].

Uwzględniając art. 32 ust. 4 ustawy o ochronie danych osobowych, należy stwierdzić, że złożony przez osobę, której dane dotyczą, wniosek

[22] Zob. art. 24 ust. 1; art. 26 ust. 1; art. 29 ust. 1; art. 30 OchrDanU.

[23] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 570; T. Szewc, *Publicznoprawna ochrona,* s. 73-74; A. Mezglewski, *Działalność związków wyznaniowych a ochrona danych osobowych,* „Studia z Prawa Wyznaniowego" 2007, t. 10, s. 9-10. Uprawnienia zakazowe P. Fajgielski nazywa też uprawnieniami szczególnymi. Por. P. Fajgielski, *Kontrola przetwarzania,* s. 145.

[24] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 74.

[25] Różnicą między obowiązkiem a uprawnieniem informacyjnym jest na przykład fakt, że informacje uzyskane przez podmiot danych mogą mieć szerszy zakres przy uprawnieniu informacyjnym niż przy obowiązku (np. uprawniony może żądać informacji o sposobie przetwarzania danych, której nie podaje się przy realizacji obowiązku informacyjnego). Do innych różnic między uprawnieniem a obowiązkiem informacyjnym możemy też zaliczyć kwestię związaną z tym, że z uprawnień informacyjnych można skorzystać wielokrotnie, a obowiązek informacyjny wyczerpuje się z chwilą zawiadomienia osoby, której dane dotyczą, o zebraniu dotyczących jej danych. Ostatnią z wymienianych w literaturze różnic między uprawieniem a obowiązkiem informacyjnym jest to, że obowiązek informacyjny jest niezależny od zamieszczenia danych w zbiorze, dla jego powstania wystarczające jest zbieranie danych, a ponadto obowiązek ten obciąża administratora „z urzędu", tzn. jest on obowiązany do poinformowania osoby, której dane dotyczą w chwili ich zbierania. Natomiast w przypadku uprawnienia informacyjnego, obowiązek podania określonych informacji powstaje z chwilą złożenia przez uprawnionego stosownego wniosku. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 74; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 572-594.

o udzielenie informacji o danych przetwarzanych w zbiorze może nie zostać przez administratora uwzględniony. Dzieje się tak w przypadku, gdy dane te przetwarzane są dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, a realizacja uprawnienia informacyjnego pociągałaby za sobą nakłady niewspółmierne z zamierzonym celem[26].

Ponadto administrator danych osobowych może nie uwzględniać wspomnianego wyżej żądania, jeśli dotyczy ono danych osobowych wykraczających poza wniosek. W odpowiedzi nie może być jednak mniej informacji niż to podano w art. 33 ust. 1 ustawy o ochronie danych osobowych. Zgodnie z brzmieniem tego przepisu, oprócz wskazania praw osoby, której dane dotyczą, należy również odpowiedzieć na następujące pytania: jakie dane osobowe zawiera zbiór (tj. jaka jest treść tych danych), w jaki sposób zebrano dane, w jakim celu i zakresie dane są przetwarzane oraz w jakim zakresie oraz komu dane zostały udostępnione. Administrator danych udziela odpowiedzi w ciągu 30 dni od otrzymania wniosku osoby, która chce skorzystać ze swoich uprawnień informacyjnych. Formę pisemną udzielenia odpowiedzi stosuje się tylko wówczas, gdy osoba, której dane dotyczą, wyraźnie tego zażąda. Udzielona na piśmie odpowiedź administratora danych musi respektować wszystkie zasady zabezpieczania danych[27].

Uprawnienia korekcyjne osoby, której dane dotyczą, stanowią realizację przewidzianego w ustawie zasadniczej uprawnienia do korygowania danych. Zgodnie z art. 51 ust. 4 obowiązującej Konstytucji RP

[26] Oznacza to, że koszty, czas, energia i nakład pracy, poświęcone na zawiadomienie, są na tyle wysokie, że oczywisty byłby brak proporcji między nakładami a celami, jakie mają być uzyskane. „Niewspółmierny" oznacza tu tyle, ile „niedający się porównać", „nieproporcjonalny". Zakłada to porównanie nakładów poniesionych na wymienione w ustawie badania naukowe, dydaktyczne, historyczne, statystyczne lub archiwalne z nakładami poniesionymi na realizację uprawnienia informacyjnego (zob. T. Szewc, *Publicznoprawna ochrona,* s. 77; A. Drozd, *Ustawa o ochronie,* s. 220-221). Szerzej na temat innych ograniczeń przy realizacji uprawnień informacyjnych przez administratora danych pisze P. Fajgielski, *Kontrola przetwarzania,* s. 154-157.

[27] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 76; G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych,* Warszawa 2003, s. 69; P. Sobczyk, *Ograniczenia praw podmiotów ze względu na przetwarzanie danych osobowych dotyczących przekonań religijnych i przynależności wyznaniowej,* „Studia z Prawa Wyznaniowego" 2010, t. 13, s. 144-145.

„każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą"[28]. Wobec powyższego uprawnienia korekcyjne zmierzają do modyfikacji sposobu postępowania administratora tak, aby było ono zgodne z zasadami przetwarzania danych osobowych[29].

O tym, które z działań korekcyjnych określonych w art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych zostanie zastosowane w konkretnym przypadku, decyduje osoba uprawniona na podstawie własnej oceny stanu faktycznego sprawy[30]. Administrator nie może zmienić wskazanego we wniosku osoby korzystającej z tych uprawnień sposobu postępowania. Zgodnie z art. 35 ust. 1 ustawy o ochronie danych osobowych administrator danych winien uwzględnić w całości wspomniane wyżej żądanie i podjąć odpowiednie działanie bez zbędnej zwłoki, jeśli tylko osoba zainteresowana wykaże (tj. udowodni), że dane osobowe, które jej dotyczą, są niekompletne (nie spełniają swojej roli z punktu widzenia celu przetwarzania), nieaktualne (nie odpowiadają rzeczywistemu stanowi rzeczy, który uległ zmianie), nieprawdziwe (nie odpowiadają rzeczywistemu stanowi rzeczy z innych przyczyn) lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla jakiego zostały zebrane[31].

Przedstawiona procedura nie ma zastosowania, gdy przepisy szczególne same regulują tryb uzupełnienia, uaktualnienia lub sprostowania[32]. W razie niedopełnienia przez administratora danych obowiązku określonego przez osobę zainteresowaną w żądaniu korekcyjnym,

---

[28] Konstytucja RP z dnia 2 kwietnia 1997 r., Dz. U. Nr 78, poz. 483 z późn. zm.

[29] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 158.

[30] Zob. A. Drozd, *Ustawa o ochronie danych,* s. 221.

[31] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 79; A. Drozd, *Ustawa o ochronie danych,* s. 245.

[32] Zob. art. 35 ust. 1 OchrDanU *in fine*. Art. 113 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z poźn. zm.) określa zasady rektyfikacji decyzji administracyjnych. Przez uzupełnienie rozumie się tutaj dodawanie informacji do danych niekompletnych w momencie pozyskania. Uaktualnienie to zmiana danych w związku z okolicznościami, które miały miejsce po ich uzyskaniu. Prostowanie zaś danych to usunięcie wszelkich błędów, usterek czy innych mylnych informacji. Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych,* s. 584; T. Szewc, *Publicznoprawna ochrona,* s. 79.

osoba ta – zgodnie z art. 35 ust. 2 ustawy o ochronie danych osobowych – może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o nakazanie dopełnienia tego obowiązku.

Ponadto art. 35 ust. 3 ustawy o ochronie danych osobowych stanowi, że jeżeli administrator danych osobowych dokona uzupełnienia, uaktualnienia czy sprostowania danych, jest zobowiązany poinformować o tym bez zbędnej zwłoki wszystkich innych administratorów, którym udostępnił zbiór danych[33].

W związku z działalnością Kościoła katolickiego w Polsce Generalnemu Inspektorowi Ochrony Danych Osobowych postawiono pytanie nawiązujące do art. 35 ust. 1 ustawy o ochronie danych osobowych. Pytanie dotyczy kwestii, czy parafianin (osoba, której dane dotyczą) ma prawo zażądać uzupełnienia danych niekompletnych lub sprostowania danych nieaktualnych zawartych w dokumentacji parafialnej. Na powyższe pytanie Inspektor odpowiada, że administrator danych ma obowiązek uwzględnić prawo osoby, której dane dotyczą, do sprostowania, jak również ich uzupełnienia w przypadku, gdy w dokumentach parafialnych przechowywane są informacje dotyczące np. nieaktualnego adresu zamieszkania, nazwiska lub numeru telefonu i innych z grupy danych zwykłych[34]. Wobec powyższego możemy stwierdzić, że osoba, której dane dotyczą, ma prawo do wglądu w jej dane osobowe zwykłe i szczególnie chronione. Na tej podstawie sugeruje się, by jednostki organizacyjne Kościoła katolickiego w Polsce były w posiadaniu dwóch odrębnych od siebie zbiorów danych: zwykłych i szczególnie chronionych. Do pierwszego z nich może mieć dostęp osoba, której dane dotyczą, realizując tym samym prawo dostępu do danych i ich uzupełniania i sprostowania zgodnie z art. 35 ust. 1 ustawy o ochronie danych osobowych. Z kolei do drugiej kategorii dostęp byłby ograniczony, a osoba zainteresowana nie mogłaby ich zmieniać w związku z zasadą autonomii i niezależności Kościoła katolickiego w Polsce i normami regulującymi tę kwestię. Autor niniejszego opracowania

[33] Obowiązek ten jest ujęty wąsko, bo powstaje tylko w przypadku udostępnienia całego zbioru danych. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 80; P. Sobczyk, *Ograniczenia praw,* s. 145-146.

[34] Zob. pyt. 14.

sugeruje, że wspomniane wyżej unormowania mogłyby się znaleźć w odrębnej Instrukcji wydanej przez administratora danych na użytek „własnego podmiotu", zgodnie z postulatem zawartym w części II ust. 5 Instrukcji kościelnej z 2009 r.

Przysługujące osobie, której dane dotyczą, uprawnienia zakazowe mogą skutkować zakazem przetwarzania danych osobowych przez administratora. Ich szczególny charakter polega również na tym, że osoba uprawniona może z nich skorzystać tylko w wyjątkowych sytuacjach, a nie zawsze (jak ma to miejsce w przypadku uprawnień informacyjnych lub korekcyjnych)[35]. Ponadto uprawnienia zakazowe stwarzają podmiotowi danych nie tylko możliwość oceny prawidłowości przetwarzania danych, ale także umożliwiają decydowanie o celach i zakresie ich przetwarzania[36].

Jednym z uprawnień zakazowych jest prawo żądania zaprzestania przetwarzania danych osoby, której one dotyczą, ze względu na jej szczególną sytuację[37]. Jeśli administrator stwierdzi, że wspomniane wyżej żądnie spełnia wymogi formalne, tj. zawiera motywację i jest ono dopuszczalne, a wskazana sytuacja jest szczególna – zgodnie z art. 32 ust. 2 ustawy o ochronie danych osobowych – zaprzestaje przetwarzania kwestionowanych danych albo bez zbędnej zwłoki przekazuje to żądanie Generalnemu Inspektorowi Danych Osobowych, który wydaje stosowną decyzję[38].

Innym uprawnieniem zakazowym, z jakiego może skorzystać osoba, której dane dotyczą, jest prawo wniesienia sprzeciwu[39]. Korzystanie z tego uprawnienia jest ograniczone przez ustawodawcę, jak przy omawianym wcześniej prawie żądania zaprzestania przetwarzania danych. Są to sytuacje określone w art. 23 ust. 1 pkt 4 i 5 ustawy o ochronie danych osobowych. Dodatkowo administrator może nie uwzględniać sprzeciwu, o którym mowa wyżej, jeżeli zamierza przetwarzać dane w celach marketingowych lub przekazywać je innemu administra-

[35] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 161.
[36] Zob. tamże, s. 163.
[37] Zob. art. 32 ust. 1 pkt 7 OchrDanU.
[38] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 81.
[39] Zob. art. 32 ust. 1 pkt 8 OchrDanU.

torowi danych[40]. Jak możemy zauważyć, w powyższym uprawnieniu zakazowym brak jest wymogu zachowania określonej formy sprzeciwu.

Po otrzymaniu wniosku, stanowiącego realizację omawianego prawa wniesienia sprzeciwu, administrator bada dopuszczalność jego złożenia. W razie stwierdzenia, że sprzeciw wniesiono z zachowaniem warunków określonych prawem, administrator – zgodnie z art. 32 ust. 3 ustawy o ochronie danych osobowych – zaprzestaje dalszego przetwarzania kwestionowanych danych[41]. Ustawa zezwala administratorowi danych jedynie na pozostawienie w zbiorze imienia lub imion i nazwiska osoby oraz numeru PESEL lub adresu wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem[42].

Ostatnie uprawnienie zakazowe, z jakiego może skorzystać osoba zainteresowana, dotyczy sytuacji, gdy osoba, której dane dotyczą, wnosi do administratora danych żądanie ponownego indywidualnego rozpatrzenia sprawy już rozstrzygniętej[43]. Oznacza to, że sprawa tej osoby została już rozstrzygnięta, ale z naruszeniem art. 26a ust. 1 ustawy o ochronie danych osobowych[44].

Zgodnie z art. 32 ust. 3a ustawy o ochronie danych osobowych, w razie wniesienia żądania przez osobę zainteresowaną i korzystającą z omawianego wyżej uprawnienia zakazowego, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasad-

[40] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 162; T. Szewc, *Publicznoprawna ochrona,* s. 82.

[41] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 82-83.

[42] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 162.

[43] Zob. Art. 32 ust. 1 pkt 9 OchrDanU.

[44] Art. 26a ust. 1 OchrDanU stanowi, że „niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym". Ustawodawcy chodzi w tym przepisie o to, by rozstrzygnięcia dotyczące osób nie były realizowane w całości przez komputery, aby zapewnić możliwość weryfikacji danego rozstrzygnięcia automatycznego przez konkretną osobę. Ustawodawca dopuścił jedynie w art. 26a ust. 2 OchrDanU rozstrzygnięcia całkowicie zautomatyzowane w przypadku, gdy rozstrzygnięcia takie podejmowane są podczas zawierania lub wykonywania umów z uwzględnieniem wniosków osób, których dane te dotyczą. Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 163.

nieniem swojego stanowiska Generalnemu Inspektorowi Ochrony Danych Osobowych, który wydaje stosowną decyzje[45].

### 3.2. OBOWIĄZKI REJESTRACYJNE

Rejestracja zbiorów danych osobowych ma umożliwić organowi ochrony danych osobowych sprawowanie uprzedniej kontroli przetwarzania danych, a jawny rejestr zbiorów tychże danych ma pozwolić wszystkim zainteresowanym na dostęp do informacji o zarejestrowanych zbiorach danych[46]. Ustawa o ochronie danych osobowych w rozdziale 6 zawiera przepisy dotyczące rejestracji zbiorów danych osobowych, stanowiąc w art. 40, że obowiązkiem administratora danych jest zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Danych Osobowych.

W art. 43 ust. 1 ustawy o ochronie danych osobowych określono zwolnienia z omawianego obowiązku rejestracji. Pośród nich uwzględniono zwolnienie z rejestracji zbioru danych osobowych, w którym zawarte są dane dotyczące osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzane na potrzeby tego kościoła lub związku wyznaniowego. Sytuacja takiego podmiotu jest uregulowana prawnie, jeżeli jest on wpisany do rejestru prowadzonego na podstawie art. 30 ustawy z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania[47] bądź jego status prawny kształtuje odrębna ustawa[48]. Uregulowaną sytuację prawną ma m.in. Kościół katolicki. Jego status określono nie tylko w ustawie z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickie-

[45] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 163. Szerzej: A. Mezglewski, *Administrowanie danymi osobowymi,* w: A. Mezglewski, H. Misztal, P. Stanisz, *Prawo wyznaniowe,* wyd. 2 rozszerzone i zaktualizowane, Warszawa 2008, s. 213-215.

[46] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 48.

[47] Dz. U. z 2005 r. Nr 231, poz. 1965 z późn. zm.

[48] Zob. T. Szewc, *Publicznoprawna ochrona,* s. 96; A. Mezglewski, *Administrowanie danymi,* s. 212; P. Sobczyk, *Ograniczenie praw,* s. 152-154.

go w Rzeczypospolitej Polskiej[49], ale również w Konkordacie między Stolicą Apostolską i Rzeczpospolitą Polską z dnia 28 lipca 1993 r.[50]

Prowadząc zbiory danych osobowych, w których zawarte są dane dotyczące należących do Kościoła katolickiego osób, Kościół katolicki w Polsce ma zagwarantowaną konstytucyjnie autonomię i niezależność (art. 25 ust. 3 Konstytucji RP). Skutkuje to wyłączeniem z obowiązku zgłaszania do rejestracji takich zbiorów przez Generalnego Inspektora Danych Osobowych. Podstawą tego zwolnienia są wskazane wyżej przepisy ustaw państwowych[51].

Wobec powyższego, trafnie wskazano w części I ust. 5 Instrukcji kościelnej z 2009 r., powołując się na wspomniany art. 43 ust. 1 pkt 3 ustawy o ochronie danych osobowych, że zbiory danych osobowych przetwarzane przez Kościół katolicki nie podlegają obowiązkowi zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Jednakże powinny one dotyczyć członków tego Kościoła i być wykorzystywane wyłącznie na jego potrzeby (np. kartoteka parafialna). W odniesieniu do tych zbiorów Inspektorowi nie przysługują uprawnienia dotyczące możliwości kontroli zgodności przetwarzania danych z ustawą o ochronie danych osobowych. Jeśli jednak przetwarzane są dane osób niebędących członkami Kościoła katolickiego, to zbiory zawierające te dane powinny być zgłaszane do rejestracji[52].

Istnienie obowiązku zgłaszania do rejestracji zbiorów danych osobowych powstałych w związku z działalnością osób prawnych Kościoła katolickiego w Polsce stało się przedmiotem pytania skierowanego do Generalnego Inspektora Ochrony Danych Osobowych. W odpowiedzi Inspektor powołuje się na art. 43 ust. 1 pkt 3 ustawy o ochronie danych osobowych i stwierdza, że o ile przetwarzanie danych następuje na potrzeby Kościoła katolickiego i dotyczy osób należących do

[49] Dz. U. Nr 29, poz. 154 z późn. zm.

[50] Dz. U. z 1998 r. Nr 51, poz. 318.

[51] Szerzej: A. Mezglewski, *Działalność związków wyznaniowych,* s. 10-15.

[52] Procedura zgłaszania zbiorów do rejestru została uregulowana w art. 41 OchrDanU. Szerzej o problematyce rejestracji zbiorów danych i wydawania zaświadczeń o funkcjach rejestracji tych zbiorów, wyłączeniach z obowiązku rejestracji, procedurze rejestracyjnej zbioru, wykreśleniu zbioru z rejestru oraz zasadzie jawności rejestru zbioru danych osobowych T. Szewc, *Publicznoprawna ochrona,* s. 95-102.

tego Kościoła, to na administratorze zbioru takich danych nie spoczywa obowiązek zgłoszenia zbioru do rejestracji. Podaje również przykłady zbiorów, które nie podlegają zgłoszeniu do rejestracji zbiorów danych osobowych. Zgodnie z omawianą odpowiedzią, nie zgłasza się np. zbiorów danych darczyńców pozostających członkami Kościoła, zbiorów danych księży, kanoników, biskupów, członków instytutów życia konsekrowanego i stowarzyszeń życia apostolskiego, zbiorów danych uczniów szkół katolickich, zbiorów danych członków Kościoła katolickiego nieuczestniczących w życiu liturgicznym tego Kościoła, zbioru danych ochrzczonych. Należy w tym miejscu zaznaczyć, że lista zbiorów niepodlegających obowiązkowi rejestracji nie jest zamknięta. W działalności Kościoła katolickiego w Polsce mogą więc być wykorzystywane także inne zbiory, które będą podlegały zwolnieniu z obowiązku rejestracyjnego. Generalny Inspektor Danych Osobowych stwierdza również, że jeżeli prowadzone przez Kościół katolicki zbiory danych osobowych dotyczą osób niebędących jego członkami, to takie zbiory podlegają zgłoszeniu na zasadach ogólnych, które określono w art. 40 ustawy o ochronie danych osobowych. Do takich zbiorów Inspektor zalicza m.in.: zbiory danych osobowych mieszkańców domów opieki społecznej prowadzonych przez zgromadzenia zakonne; zbiory danych osobowych darczyńców nienależących do Kościoła katolickiego; zbiory danych osób, którym udzielane jest wsparcie lub pomoc (np. ewidencja bezdomnych korzystających z noclegowni prowadzonych przez Caritas)[53].

Inne pytanie kierowane do Generalnego Inspektora Danych Osobowych dotyczyło, gdzie można uzyskać informację o zbiorach zgłoszonych do rejestracji przez Kościół katolicki. W odpowiedzi na nie Inspektor stwierdza, że w celu realizacji postanowień art. 12 pkt 3 i art. 42 ust. 1 ustawy o ochronie danych osobowych to właśnie do jego kompetencji należy prowadzenie ogólnokrajowego, jawnego rejestru zbiorów danych osobowych oraz udzielanie informacji o zarejestrowanych zbiorach, między innymi za pośrednictwem strony internetowej (www.giodo.gov.pl)[54].

[53] Zob. pyt. 2.
[54] Zob. pyt. 3.

### 3.3. OBOWIĄZKI ZABEZPIECZANIA DANYCH

Obowiązki administratora danych związane z zabezpieczaniem danych osobowych[55] wylicza art. 36 ust. 1 ustawy o ochronie danych osobowych. Przepis ten stanowi: „administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem".

Obowiązki administratora danych związane z zabezpieczaniem danych wiążą się ściśle z realizacją zasady poufności. Obowiązki te odnoszą się do organizacyjnych i technicznych aspektów przetwarzania danych i nakazują zachowanie danych w tajemnicy wobec osób, które nie są uprawnione do dostępu do danych 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 zagwarantowanie należytego zabezpieczania przetwarzanych danych, gdyż nawet najlepsze regulacje prawne nie zapewnią skutecznej ochrony w sytuacji, gdy rozwiązania techniczne i organizacyjne będą nieodpowiednie. Wszystkie mechanizmy zabezpieczania danych powinny być proporcjonalne do zagrożeń i kategorii przetwarzania danych[56].

---

[55] Pod pojęciem „zabezpieczanie 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 prawnoporównawcza,* Toruń 1981, s. 25; P. Fajgielski, *Kontrola przetwarzania,* s. 35-36). Problematyka zabezpieczania danych osobowych została szczegółowo uregulowana w przepisach rozdziału piątego OchrDanU oraz w rozporządzeniu wykonawczym do tej ustawy – zob. rozporządzenie 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. Nr 100, poz. 1024.

[56] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 48.

Do obowiązków związanych z zabezpieczaniem danych osobowych przez administratora danych nawiązuje Instrukcja kościelna z 2009 r. W części II, ust. 2 Instrukcja stanowi, że administrator ma obowiązek zabezpieczyć te dane poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, tak aby: 1) nie były udostępniane osobom nieupoważnionym; 2) nie były zabrane przez osobę nieuprawniona oraz 3) były zabezpieczone przed uszkodzeniem, zniszczeniem lub utratą[57]. Ponadto Instrukcja ta, nawiązując do art. 36 ust. 1 ustawy o ochronie danych osobowych, wylicza enumeratywnie obowiązki administratora związane z zabezpieczaniem danych osobowych, choć jak zauważamy, ustawowe obowiązki administratora w tej dziedzinie są wymienione przykładowo, na co wskazuje użyte w ustawie wyrażenie: „w szczególności"[58]. Wydawałoby się rzeczą wskazaną, by także w Instrukcji kościelnej z 2009 r. nie zawężać katalogu obowiązków administratora danych, bo rozwiązania techniczne i organizacyjne muszą być dostosowywane do postępów informatycznych.

Do innych obowiązków administratora dotyczących prawidłowego zabezpieczania danych osobowych zalicza się także obowiązek dołożenia szczególnej staranności przy przetwarzaniu i należytym zabezpieczaniu danych. Obowiązek ten ma na celu ochronę interesów osób, których dane dotyczą. Ustawa o ochronie danych osobowych ściśle łączy realizację tego obowiązku z respektowaniem podstawowych zasad odnoszących się do jakości danych (legalności, celowości, prawdziwości, adekwatności i ograniczenia czasowego przetwarzania danych). Do tego ogólnego obowiązku dołożenia szczególnej staranności przy przetwarzaniu danych osobowych dodaje się obowiązki szczegółowe wobec administratora danych. Do nich zalicza się: obowiązek informacyjny, mający na celu informowanie o osobach przetwarzających dane osobowe, fakcie, treści, zakresie i celu przetwarzania danych, a także obowiązek korekcyjny (rektyfikacyjny), który zmierza do poprawiania danych nieprawidłowych[59].

---

[57] Zob. część II ust. 2 *in fine* Instrukcji kościelnej.

[58] Instrukcja kościelna z 2009 r. nie wylicza m.in. przetwarzania danych z naruszeniem (ustawy) prawa i zmiany danych osobowych.

[59] Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 46-48; A. Mezglewski, *Administrowanie danymi,* s. 212.

Kolejnym obowiązkiem związanym z zabezpieczaniem danych osobowych i spoczywającym na administratorze tychże danych jest kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane[60]. W zakresie obowiązku związanego z kontrolą przetwarzania i ochrony danych osobowych przepisy ustawy nakładają na administratora wiele szczegółowych obowiązków. Należą do nich m.in.: obowiązek wyznaczenia administratora bezpieczeństwa inforamcji[61], obowiązek wdrożenia dokumentacji opisującej sposób przetwarzania danych i środki zabezpieczenia danych[62] oraz obowiązek nadawania upoważnień do przetwarzania danych i prowadzenia ewidencji osób upoważnionych[63].

Istnieje jeszcze wiele innych obowiązków administratora danych związanych z zabezpieczaniem danych osobowych oraz ich ochroną, wynikających bezpośrednio z ustawy o ochronie danych osobowych. Obowiązki nie są związane bezpośrednio z osobą administratora danych osobowych, stąd nie wydaje się uzasadniona w tym miejscu ich szczegółowa analiza[64].

### 3.4. OBOWIĄZKI WYNIKAJĄCE BEZPOŚREDNIO Z UNORMOWAŃ KOŚCIELNYCH

Instrukcja kościelna z 2009 r. w części II ust. 6 podaje obowiązki administratora danych wynikające z Kodeksu Prawa Kanonicznego z 1983 r.[55] Powołując się na kan. 486-491 KPK/83, w Instrukcji określono zasady dotyczące archiwizacji dokumentów, tym samym

[60] Zob. Art. 38 OchrDanU.

[61] Zob. Art. 36 ust. 3 OchrDanU.

[62] Zob. Art. 36 ust. 2 OchrDanU.

[63] Zob. Art. 37 OchrDanU. Zgodnie z art. 39 OchrDanU, administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator (jeżeli dane są przetwarzane w systemie informatycznym). Natomiast osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia. Zob. P. Fajgielski, *Kontrola przetwarzania,* s. 48-49.

[64] Obowiązki podmiotów przetwarzających dane osobowe zostały trafnie zebrane i pogrupowane w rozprawie P. Fajgielskiego *Kontrola przetwarzania,* s. 46-49.

regulując kwestie zabezpieczania danych osobowych w Kościele katolickim[66].

Prawodawca kościelny w kan. 486 KPK/83 nakazuje, by z największą troską strzec wszystkich dokumentów dotyczących diecezji i parafii. Ponadto w każdej kurii, w miejscu bezpiecznym, winno się urządzić archiwum diecezjalne, czyli depozyt dokumentów, w którym winny być przechowywane dokumenty i pisma dotyczące spraw diecezjalnych – zarówno duchownych, jak i doczesnych – odpowiednio uporządkowane i pilnie strzeżone pod zamknięciem. Należy także sporządzić inwentarz, czyli katalog dokumentów znajdujących się w archiwum, z dołączeniem krótkiego opisu każdej pozycji.

Wspomniane archiwum winno być zamknięte, a klucz od niego winien mieć tylko biskup i kanclerz. Nikomu też nie wolno wchodzić do tego archiwum bez zezwolenia biskupa lub moderatora kurii i kanclerza równocześnie (kan. 487 KPK/83).

Dokumenty tajne winno się przechowywać z największą pilnością w kurii diecezjalnej, w tajnym archiwum lub przynajmniej w ogólnym archiwum, gdzie winna się znajdować kasa pancerna, dobrze zamknięta i umocowana, której nie da się wynieść z miejsca. Ponadto każdego roku należy niszczyć dokumenty spraw karnych w zakresie obyczajów, dotyczące osób zmarłych albo spraw zakończonych przed dziesięciu laty wyrokiem skazującym, zachowując krótkie streszczenie faktu wraz z tekstem wyroku (kan. 489 KPK/83)[67].

Natomiast Instrukcja kościelna z 2009 r. poświęca właściwemu zabezpieczaniu danych osobowych przez administratorów całą cześć II składającą się z sześciu ustępów. W celu zabezpieczania danych osobowych przez jednostki organizacyjne Kościoła katolickiego

---

[65] *Codex Iuris Canonici auctoritate Ioannis Pauli PP.II promulgatus, Kodeks Prawa Kanonicznego, przekład polski zatwierdzony przez Konferencję Episkopatu Polski,* Pallottinum, Poznań 1984 [dalej: KPK/83]. Szerzej na temat unormowań prawa kanonicznego, które odnoszą się do ochrony danych osobowych, zob.: A. Mezglewski, *Działalność związków wyznaniowych,* s. 17-18.

[66] P. Sobczyk, *Ograniczenie praw,* s. 147. Szerzej: P. Majer, *Ochrona prywatności w kanonicznym porządku prawnym,* w: *Ochrona danych osobowych i prawo do prywatności w Kościele,* red. P. Majer, wyd. 2, Kraków 2002, s. 83-123.

[67] Zob. część II ust. 6 Instrukcji kościelnej.

w Polsce wprowadza ona zasadę ogólną. W Instrukcji (część II ust. 1) wyjaśniono, iż podane przez prawo (tj. m.in. przez Konstytucję RP oraz ustawę o ochronie danych osobowych) liczne ograniczenia możliwości ingerencji Generalnego Inspektora Danych Osobowych w sferę danych zbieranych w ramach Kościoła katolickiego nie oznaczają zwolnienia ze staranności w zabezpieczaniu zbieranych danych przed dostępem do nich innych osób nieuprawnionych. Nie wiążą się też ze swobodą w rozpowszechnianiu bądź przekazywaniu zebranych danych innym instytucjom lub osobom. Chociaż Kościół katolicki ma prawo przetwarzać dane osobowe dla realizacji swojej działalności statutowej, to przetwarzanie tych danych powinno odbywać się z poszanowaniem godności jednostki.

Kolejno, w części II ust. 3 pkt 1-3 Instrukcji kościelnej z 2009 r., podano praktyczne wskazówki, którymi należy się kierować przy zabezpieczaniu danych osobowych gromadzonych w związku z działalnością Kościoła katolickiego. Zgodnie z nimi istotnym jest tu zabezpieczenie obszaru, w którym przetwarzane są dane osobowe w formie papierowej lub w systemie informatycznym, a więc zabezpieczenie budynku, pomieszczenia lub części pomieszczeń, gdzie przetwarzane są te dane (pkt 1). Istotne znaczenie posiada ponadto zabezpieczenie dokumentów zawierających dane osobowe (pkt 2) oraz zabezpieczenie systemów informatycznych służących do przetwarzania danych osobowych (pkt 3).

Instrukcja zawiera ponadto szczegółowe dyspozycje odnoszące się do jednostek organizacyjnych Kościoła katolickiego w Polsce, którymi należy się kierować, zabezpieczając obszar, gdzie są przetwarzane dane (zob. część II ust. 3 pkt 1 Instrukcji kościelnej). Są nimi: zastosowanie odpowiednich zamków, drzwi, systemów alarmowych itp., zapewnienie kluczy do pomieszczeń, szaf, biurek itp. oraz kontroli ich używania oraz zabezpieczenie przed dostępem osób trzecich na czas nieobecności w pomieszczeniach osób upoważnionych.

Omawiany dokument zawiera także szczegółowe wskazania odnośnie do zabezpieczania danych osobowych przetwarzanych w sposób tradycyjny (manualny, papierowy), czyli zabezpieczenie dokumentów zawierających te dane. W części II ust. 3 pkt 2 Instrukcji podano, iż zabezpieczenie takich dokumentów winno uwzględniać: zapewnienie dostępu do dokumentów wyłącznie osobom upoważnio-

nym, zobligowanym do zachowania w tajemnicy pozyskanej informacji; niszczenie dokumentów zbędnych w sposób uniemożliwiający odtworzenie danych znajdujących się w tych dokumentach oraz przechowywanie dokumentów w zamkniętych na klucz szafach po zakończeniu pracy.

Autorzy Instrukcji kościelnej z 2009 r. sformułowali także praktyczne wskazówki dotyczące zabezpieczania danych osobowych w systemach informatycznych (w postaci elektronicznej, przy użyciu np. komputera, laptopa). Stąd w części II ust. 3 pkt 3 Instrukcji wskazano, że zabezpieczanie systemów informatycznych służących do przetwarzania danych osobowych winno się odbywać przez: zapewnienie dostępu do komputerów wyłącznie osobom upoważnionym (np. ustawienie monitorów komputerowych w sposób uniemożliwiający osobom postronnym zapoznanie się z danymi, zachowanie w tajemnicy haseł dostępu do komputerów, zastosowanie wygaszacza ekranu w momencie niekorzystania z komputera), a także przechowywanie elektronicznych nośników informacji zawierających dane osobowe (dyskietki, płyty CD, taśmy magnetyczne) w sposób zabezpieczający przed nieupoważnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem. W sytuacji gdy dane osobowe przetwarzane są na komputerze przenośnym (laptopie), to niezbędne jest zachowanie szczególnej ostrożności podczas transportu, przechowywania i użytkowania w terenie oraz zastosowanie programu szyfrującego. Ponadto systemy informatyczne, przy użyciu których przetwarzane są dane osobowe, zabezpiecza się przed utratą zasilania poprzez zastosowanie urządzeń UPS oraz poprzez wykonywanie okresowych kopii bezpieczeństwa. Natomiast wobec zagrożeń pochodzących z sieci publicznej Internet zabezpiecza się je za pomocą specjalistycznych mechanizmów teleinformatycznych, takich jak: zapora ogniowa (tzw. firewall), system wykrywania włamań czy oprogramowanie antywirusowe. Zagrożenia powyższe, jak wskazano w Instrukcji, można wyeliminować poprzez korzystanie z komputera niemającego połączenia z Internetem. Generalizując przedstawione uwagi, w Instrukcji zwrócono uwagę, że każdy z wymienionych wyżej rodzajów zabezpieczeń należy dostosować do rodzaju zagrożeń i kategorii przetwarzanych danych osobowych. Zachowanie należytej staranności w procesie przetwarzania tych danych może przejawiać się

przykładowo w wyeliminowaniu przypadków umieszczania dokumentów w miejscach ogólnie dostępnych lub w otwartych szafach.

W tym miejscu warto dodać, że istnieją różne środki zabezpieczeń w systemie informatycznym. Rzeczą wskazaną jest, by jednostki organizacyjne Kościoła katolickiego w Polsce zastosowały je w praktyce w postaci aktów normatywnych lub decyzji administracyjnych[68].

W omawianej Instrukcji określono również ogólne zasady, którymi winni się kierować kościelni administratorzy danych osobowych w Polsce dla zachowania bezpieczeństwa przy użytkowaniu Internetu (część II ust. 4). Zasad tych nie wyliczono jednak taksatywnie, na co wskazuje wyrażenie: „w szczególności"[69]. Instrukcja podaje więc, że nie należy otwierać plików pochodzących od nieznanego nadawcy, nie należy też uruchamiać ani zgrywać na twardy dysk komputera żadnych nielegalnych programów czy plików pobranych z niewiadomego źródła. Dla zabezpieczenia przed szkodliwym oprogramowaniem infekującym w sposób automatyczny system operacyjny komputera nie należy otwierać stron, na których prezentowane są informacje o charakterze przestępczym, hakerskim, nie należy również w przeglądarce internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł. Na bieżąco należy aktualizować system operacyjny komputera, system antywirusowy, jak również system firewall. Omawiany wątek kończy przestroga, że nikt nie jest w sieci anonimowy, a korzystanie z każdej strony „www" jest utrwalane i może być wykorzystywane przez różne podmioty dla celów często niezgodnych z prawem.

Jak wynika z powyższego omówienia, duża część wskazań zawartych w Instrukcji kościelnej z 2009 r. została podana w celu zabezpieczania danych przetwarzanych w systemach informatycznych (zob. część II ust. 3 pkt 3 i 4 Instrukcji kościelnej). Jest to niewątpliwie rzeczą słuszną ze względu na rosnący rozwój technologii informatycznych i komunikacyjnych oraz związane z nim zagrożenia, a także z uwagi na fakt, że tradycyjny system zabezpieczania danych osobowych został już uregulowany w KPK/83.

---

[68] Szerzej na ten temat: T. Szewc, *Publicznoprawna ochrona,* s. 57-72.

[69] Zob. część II ust. 4 Instrukcji kościelnej.

Obowiązku zabezpieczania danych osobowych przez administratora danych dotyczy kilka pytań, które skierowano do Generalnego Inspektora Ochrony Danych Osobowych w związku z działalnością Kościoła katolickiego w Polsce. I tak pojawiło się pytanie, czy proboszcz może przekazać informacje o osobach zamierzających wstąpić w związek małżeński podmiotom trzecim świadczącym usługi (np. salonowi sukien ślubnych, fotografowi, kwiaciarni). Generalny Inspektor Ochrony Danych Osobowych w odpowiedzi na nie przytacza omawiany wyżej art. 36 ustawy o ochronie danych osobowych. Przypomnijmy, że zgodnie z tym przepisem administrator danych osobowych – w tym także proboszcz – jest zobowiązany zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną czy przetwarzaniem z naruszeniem ustawy. Stąd „proboszcz nie może udostępniać danych pozyskanych w celu udzielenia sakramentu, w innych celach, osobom trzecim”[70].

Generalnemu Inspektorowi Ochrony Danych Osobowych postawiono również pytanie o to, kto sprawuje pieczę nad danymi osobowymi zgromadzonymi w księgach parafialnych. Odpowiedź Inspektora bazuje na KPK/83, gdzie zgodnie z kan. 535 KPK/83 proboszcz ma czuwać nad tym, by księgi parafialne były właściwie spisywane i przechowywane[71].

Za trafne należy uznać zalecenie, aby administrator danych opracował pisemną instrukcję dotyczącą sposobu zarządzania, ochrony i wymiany informacji (danych osobowych) w systemie tradycyjnym (papierowym) oraz informatycznym wewnątrz swojej jednostki (część II ust. 5 Instrukcji kościelnej). Wydanie takiej instrukcji na użytek wewnętrzny danej jednostki organizacyjnej pozwoli na prawidłowe zarządzanie danymi osobowymi. Ponadto jak wskazuje się w Instrukcji, uzasadnionym wydaje się także wyznaczenie osoby, która będzie odpowiedzialna za właściwe stosowanie opracowanych przez administratora danych reguł. Jest to szczególnie ważne, gdy dostęp do danych osobowych poza administratorem mają inne osoby. Wydaje się więc wskazaną rzeczą, by powstały takie instrukcje na użytek „własne-

[70] Zob. pyt. 7.
[71] Zob. pyt. 11.

go podmiotu", a także wyznaczane były przez administratora danych odrębne osoby, które by były odpowiedzialne za właściwe stosowanie opracowanych na użytek wewnętrzny reguł.

## 5. ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW USTAWY

Ważne miejsce wśród unormowań określających pozycję prawną administratora danych osobowych zajmują regulacje odnoszące się do jego odpowiedzialności za naruszenie przepisów ustawy o ochronie danych osobowych. Możemy tu mówić o odpowiedzialności w aspekcie: administracyjnym[72], cywilnym[73], pracowniczym[74] i karnym[75]. W ustawie o ochronie danych osobowych (a dokładniej – w jej rozdziale 8) uregulowano jedynie kwestie związane z odpowiedzialnością o charakterze prawnokarnym. W art. 49-54 tego aktu normatywnego zostały określone przestępstwa, jakie może popełnić administrator danych. Należą do nich: nielegalne przetwarzanie, naruszenie zasady związania celem, udostępnienie danych osobom nieuprawnionym, naruszenie zasad bezpieczeństwa, niezgłoszenie zbioru danych do rejestru oraz niewykonanie obowiązku informacyjnego[76]. Przestępstwa te ścigane są z oskarżenia publicznego. Można je popełnić umyślnie (tzn. sprawca chce ich popełnienia lub przewidując taką możliwość, na to się godzi), chyba że

[72] Wyraża się ona w możliwości wydania przez Generalnego Inspektora Danych Osobowych jednej z decyzji zmierzających do przywrócenia stanu zgodnego z prawem. Zob. T. Szewc, *Publicznoprawna ochrona,* s. 92-94.

[73] Jej zaistnienie jest zależne od naruszenia jednej z przesłanek odpowiedzialności deliktowej (art. 415 KC), kontraktowej (art. 471 KC) lub z tytułu naruszenia dóbr osobistych (art. 23-24 KC).

[74] Zachodzi ona, jeżeli wypełnione są przesłanki odpowiedzialności porządkowej, dyscyplinarnej, ewentualnie materialnej odpowiedzialności pracownika względem pracodawcy. Podstawę prawną stanowi ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy, Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.

[75] Występuje ona, jeżeli działanie sprawcy wypełnia znamiona czynów zabronionych stypizowanych w art. 49 i n OchrDanU przy uwzględnieniu norm prawnokarnych zawartych w rozdziale XXXIII („Przestępstwa przeciwko ochronie informacji" – art. 265-269b) ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. Nr 88, poz. 553 z późn. zm.

[76] Zob. A. Mezglewski, *Działalność związków wyznaniowych,* s. 10.

w ustawie zaznaczono inaczej[77]. Osobom naruszającym prawnokarne przepisy ustawy o ochronie danych osobowych grożą – w zależności od popełnionego przestępstwa – następujące sankcje: grzywna, kara ograniczenia wolności lub kara pozbawienia wolności do lat 3[78].

## PODSUMOWANIE

Kwestię ochrony danych osobowych w Kościele katolickim regulują przede wszystkim przepisy ustawy o ochronie danych osobowych. One też określają pozycję prawną administratora danych osobowych. Ważne znaczenie w zakresie zabezpieczania i przetwarzania danych osobowych przez jednostki organizacyjne Kościoła katolickiego w Polsce ma również Kodeks Prawa Kanonicznego oraz Instrukcja kościelna z 2009 r. Jej przyjęcie przyczyni się z pewnością do uporządkowania praktyki przetwarzania danych w Kościele. W Instrukcji podzielono bowiem obowiązki obciążające kościelnych administratorów danych na te, które wynikają z ustawy o ochronie danych osobowych oraz te, które znajdują swe źródło w prawie kanonicznym. Trafnie wskazano w niej również na potrzebę opracowania przez administratorów danych odrębnej instrukcji, która – na użytek określonego podmiotu – jeszcze precyzyjniej dookreślałaby zasady zabezpieczania danych osobowych. Wydanie takiej instrukcji na użytek wewnętrzny danej jednostki organizacyjnej pozwoli na prawidłowe zarządzanie danymi osobowymi. Mimo że w żadnym miejscu Instrukcja nie wskazuje na możliwość czy konieczność wyznaczenia osoby administratora bezpieczeństwa informacji, która nadzorowałaby przestrzeganie zasad ochrony danych osobowych, to analiza wielu obowiązków administratora danych skłania do jej ustanowienia w jednostkach organizacyjnych Kościoła katolickiego w Polsce. Pojawienie się administratora bezpieczeństwa informacji zwiększyłoby poczucie bezpieczeństwa związanego z ochroną danych osobowych przetwarza-

[77] Na przykład przestępstwo naruszenia zasad bezpieczeństwa związanych z zabezpieczaniem danych osobowych popełnione przez administratora danych osobowych jest możliwe nie tylko z winy umyślnej, ale także i nieumyślnej (art. 52 OchrDanU).

[78] Szerzej na ten temat: T. Szewc, *Publicznoprawna ochrona,* s. 103-108.

nych przez Kościół katolicki. Jest to szczególnie ważne, gdy dostęp do danych osobowych poza administratorem mają inne osoby.

## PROTECTION OF PERSONAL DATA IN THE ACTIVITY OF THE ROMAN CATHOLIC CHURCH IN POLAND


### Summary

Adequate protection of personal data in the activity of the Roman Catholic Church in Poland raises many questions and arouses controversy. This article addresses the following questions: who is the administrator of personal data in the Catholic Church; what are his responsibilities; what is his liability for failing to protect such data.

The idea of the personal data administrator in the organizational units of the Catholic Church in Poland goes back to the Act of 29 August 1997 on the Protection of Personal Data. The administrator of personal data is an entity, in this case the Catholic Church, that determines the purposes and means of processing personal data; such an administrator may also authorize another entity for such processing.

The paper discusses the requirements as to the disclosure, registration and security of personal data, which should be met by the administrator. In addition, the author touches upon the relevant obligations arising directly from the 1983 Code of Canon Law and the Instruction of 23 September 2009 on the protection of personal data in the activity of the Roman Catholic Church in Poland issued by the Polish Episcopal Conference.

*Translated by Konrad Szulga*