Ważny krok dla naszej wspólnoty

Posted on 2025-11-28

O ochronie danych osobowych w Kościele prawosławnym, o cyberbezpieczeństwie w jego strukturach, a także o współpracy między tym Kościołem a Prezesem UODO w ramach niedawno podpisanego porozumienia – z ks. Andrzejem Lewczakiem, Kościelnym Inspektorem Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego, rozmawia Karol Witowski.

W jaki sposób porozumienie z Prezesem UODO może się przyczynić do wzmocnienia systemu ochrony danych osobowych w Polskim Autokefalicznym Kościele Prawosławnym?

To ważny krok dla Polskiego Autokefalicznego Kościoła Prawosławnego. Podpisane 15 października 2025 r. porozumienie otwiera Kościołowi prawosławnemu drogę do stałej współpracy merytorycznej i edukacyjnej z krajowym organem nadzoru. Dzięki temu możemy liczyć na dostęp do aktualnych materiałów szkoleniowych i praktycznych wytycznych, eksperckie wsparcie przy interpretacji przepisów w kontekście specyfiki kościelnej, wspólne działania informacyjne skierowane do duchownych i wiernych, a także – w razie potrzeby – na szybszą ścieżkę konsultacyjną w procesie przygotowywania wewnętrznych procedur. W efekcie zwiększa to spójność podejścia w całej strukturze Kościoła i podnosi standard ochrony danych na poziomie parafii i diecezji.

Jakie są główne wyzwania w strukturze Kościoła prawosławnego, które przekładają się na potencjalne problemy w obszarze ochrony danych osobowych?

Najważniejsze wyzwania to rozproszenie organizacyjne (wiele parafii i jednostek o różnym stopniu dostosowania do wymogów prawnych), zróżnicowane systemy dokumentacji (papierowe i elektroniczne), duża rola dokumentów historycznych i rejestrów parafialnych, częste angażowanie osób niebędących pracownikami do przetwarzania danych oraz ograniczone zasoby IT i kadrowe w mniejszych parafiach/jednostkach.

Dochodzą do tego specyficzne praktyki duszpasterskie – np. prowadzenie ksiąg chrztów czy małżeństw – które wymagają szczególnej uwagi przy określaniu podstaw prawnych i sposobów zabezpieczenia danych.

Jaki jest podstawowy paradygmat ochrony danych w Kościele prawosławnym?

Można go ująć w trzech filarach: świadomość duszpasterska, zasada proporcjonalności oraz decentralizacja odpowiedzialności przy centralnym wsparciu. Oznacza to, że ochrona danych jest traktowana jako element posługi duszpasterskiej, przetwarzamy tylko dane niezbędne, a każda jednostka (parafia, diecezja) ponosi odpowiedzialność za własne operacje, mając jednocześnie dostęp do wytycznych, procedur i wsparcia KIODO na poziomie centralnym. W praktyce obejmuje to wzory polityk, instrukcji i klauzul informacyjnych, szkolenia oraz zalecenia dotyczące przechowywania dokumentów i zabezpieczeń technicznych.

A jak wygląda system obiegu dokumentów między diecezjami?

Obieg ma charakter hybrydowy. Wiele dokumentów funkcjonuje w formie papierowej i jest przechowywanych lokalnie, a część administracyjno-kadrowa – równolegle w formie elektronicznej. Przekazywanie dokumentów między diecezjami odbywa się przede wszystkim poprzez oficjalną korespondencję pocztową oraz zaszyfrowane załączniki e-mail. KIODO promuje minimalizację przesyłanych danych oraz obowiązek szyfrowania danych przesyłanych drogą elektroniczną.

Na co dzień Kościół prawosławny musi też na pewno rozwiązywać problem z transferem danych do państw trzecich – to przykład diecezji w Brazylii, która podlega PAKP.
Tak, diecezja w Brazylii podlega jurysdykcji Kościoła prawosławnego w Polsce, co wymusza analizę zarówno praktycznych, jak i prawnych aspektów przekazywania danych. Ponieważ Brazylia nie znajduje się w obszarze stosowania RODO, konieczne jest zapewnienie odpowiedniej podstawy prawnej i adekwatnych zabezpieczeń. W praktyce ograniczamy transfery do danych niezbędnych z perspektywy działań duszpasterskich i administracyjnych, stosując m.in. szyfrowanie.

Czy jednostki Kościoła są celem cyberataków, jak Kościół sobie z tym radzi?
Tak, podobnie jak inne podmioty publiczne i niepubliczne, parafie oraz instytucje kościelne stają się celem phishingu, malware czy ataków na pocztę e-mail.

Nasza reakcja opiera się na podstawowych zabezpieczeniach technicznych (aktualizacje, antywirusy, zapory), szkoleniach i działaniach podnoszących świadomość użytkowników oraz na procedurach reagowania na incydenty. Nie dysponujemy jednym centralnym systemem, dlatego promujemy zestaw prostych i skutecznych dobrych praktyk, dostosowanych do możliwości mniejszych jednostek.

Jakie są obecnie największe wyzwania dotyczące ochrony danych w Kościele prawosławnym i jak je osadzić w kontekście wsparcia Prezesa UODO?

Do najważniejszych wyzwań zaliczamy: ujednolicenie standardów w rozproszonej strukturze, rozwój kompetencji IT w parafiach, właściwe uregulowanie transferów międzynarodowych oraz edukację duchowieństwa i wolontariuszy. Prezes UODO może wesprzeć te działania poprzez dostarczanie przystępnych materiałów oraz wzorów procedur uwzględniających specyfikę kościelną, wsparcie szkoleniowe (w tym programy dedykowane), udostępnienie szybkiej ścieżki konsultacyjnej, a także – jeśli to możliwe – inicjatywy wspierające mniejsze jednostki w pozyskiwaniu podstawowych narzędzi IT i zabezpieczeń.

Czy Kościół prowadził działania informacyjne dla duchownych i wiernych?

Tak, działania informacyjne były i są realizowane na kilku poziomach: poprzez materiały informacyjne i zalecenia (instrukcje, broszury), szkolenia dla duchowieństwa i pracowników parafii, konferencje diecezjalne oraz komunikaty dla wiernych publikowane na stronach parafialnych i w ogłoszeniach. Proces ten rozwijał się stopniowo. Większe ośrodki mają bardziej rozbudowane programy szkoleniowe, natomiast mniejsze parafie częściej opierają się na materiałach centralnych. Porozumienie z UODO pozwoli ten proces uporządkować i rozszerzyć.

Czy technologie sztucznej inteligencji pomagają w misji religijnej?

Wykorzystanie AI wymaga dużej ostrożności – zwłaszcza w zakresie prywatności, przejrzystości działania algorytmów oraz ryzyka błędnych rekomendacji. Jesteśmy na etapie analiz i obserwacji możliwych zastosowań.

Czy Kościół prawosławny otrzymuje wsparcie od instytucji europejskich?

Obecnie nie korzystamy z takiego wsparcia. Główne działania realizowane są na bazie inicjatyw krajowych oraz współpracy z krajowym organem nadzoru. Korzystamy przede wszystkim z uniwersalnych wytycznych, materiałów edukacyjnych oraz decyzji organów ochrony danych, które kształtują ramy prawne i praktyczne.

Dziękuję za rozmowę