POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Wspólnota Życia Chrześcijańskiego w Polsce

Adres siedziby: 02-532 Warszawa, ul. Rakowiecka 61

Celem Polityki bezpieczeństwa danych osobowych, zwanej dalej „Polityką", jest wprowadzenie i utrzymanie właściwej ochrony bezpieczeństwa danych osobowych, w związku z przetwarzaniem danych osobowych przez Wspólnotę Życia Chrześcijańskiego w Polsce na podstawie przepisów:

- *Dekretu ogólnego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydanego przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r.* (zwanego dalej „Dekretem") - w przypadkach związanych z misją Kościoła i wykonywaniem wewnętrznych zadań Kościoła objętych, co do zasady, prawem kanonicznym, oraz
- *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, Dz. Urz. UE.L Nr 119, str. 1 ze sprost. (zwanym dalej „RODO") - w przypadkach wykraczających poza misję Kościoła,

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych (w postaci papierowej), jak i w systemach informatycznych, w tym na informatycznych nośnikach danych (w postaci elektronicznej). Dotyczy danych osobowych oraz ich zbiorów istniejących oraz przetwarzanych obecnie i w przyszłości.
Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych we Wspólnocie Życia Chrześcijańskiego w Polsce.

W skład obszaru przetwarzania danych osobowych we Wspólnocie Życia Chrześcijańskiego w Polsce wchodzą budynki i lokale położone w Warszawie przy ul. Rakowieckiej 61 oraz w:

- Białymstoku, ul. Południowa 31, 15-341 Białystok (Dom Księży Jezuitów w Białymstoku),
- Gdyni, ul. Tatrzańska 35, 81-313 Gdynia (ICFD),
- Kaliszu, ul. Stawiszyńska 2, 62-800 Kalisz (Sanktuarium Serca Jezusa Miłosiernego w Kaliszu),
- Krakowie, ul. Kopernika 26, 31-501 Kraków (Zgromadzenie zakonne Księży Jezuitów),
- Lublinie, ul. Radziszewskiego 7, 20-031 Lublin (Sekretariat DA KUL),
- Łodzi, ul. Sienkiewicza 60, 90-058 Łódź (Parafia Najświętszego Imienia Jezus),
- Piotrkowie Trybunalskim, ul. Pijarska 47 97-300 Piotrków Trybunalski (Sanktuarium Matki Bożej Trybunalskiej),
- Poznaniu, ul. Szewska 18a, 61-760 Poznań (Zgromadzenie zakonne Księży Jezuitów),
- Radomiu, ul. Tybla 4 26-600 Radom (Zgromadzenie zakonne Księży Jezuitów),
- Szczecinie, ul. Pocztowa 22, 70- 345 Szczecin (Zgromadzenie zakonne Księży Jezuitów),
- Toruniu, ul. Piekary 24, 87-100 Toruń (Zgromadzenie zakonne Księży Jezuitów),
- Wrocławiu, ul. Wincentego Stysia 16, 53-526 Wrocław (Zgromadzenie zakonne Księży Jezuitów)

§ 1.
Definicje

Użyte w Polityce określenia oznaczają:

1) Administrator Danych Osobowych (ADO) – Wspólnota Życia Chrześcijańskiego w Polsce;
2) przedstawiciel Administratora Danych Osobowych – prezydent Wspólnoty Życia Chrześcijańskiego w Polsce;
3) Inspektor Ochrony Danych (IOD) – osoba fizyczna lub zespół osób wyznaczonych przez ADO;
4) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) przetwarzanie danych osobowych – czynności wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, archiwizowanie;
6) Wspólnota Życia Chrześcijańskiego – Wspólnota Życia Chrześcijańskiego w Polsce, zwana dalej „WŻCh";
7) Koordynator Lokalny (KL) – koordynuje życie wspólnoty lokalnej i reprezentuje ją na zewnątrz;
8) użytkownik – osoba upoważniona do przetwarzania danych osobowych;
9) system informatyczny – system (urządzenia, narzędzia, programy), w którym przetwarzane są dane osobowe;
10) zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

§ 2.
Zasady przetwarzania danych osobowych

1. ADO przetwarza dane osobowe:
   1) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   2) zbiera je w konkretnych, jasno określonych i prawnie uzasadnionych celach oraz nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu");
   3) adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
   4) prawidłowo, w razie potrzeby uaktualniając zebrane dane („prawidłowość");
   5) przechowując je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których te dane są przetwarzane („ograniczenie przechowywania");
   6) w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność lub poufność").

2. W celu realizacji zasad, o których mowa w ust. 1, ADO przetwarza dane osobowe legalnie, na podstawie przesłanek opisanych w art. 7 Dekretu ogólnego, w przypadkach związanych

z misją Kościoła i wykonywaniem wewnętrznych zadań Kościoła objętych, co do zasady, prawem kanonicznym albo art. 4 RODO w przypadkach wykraczających poza misję Kościoła. Pobiera dane adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza, wypełnia obowiązki informacyjne określone w art. 8 lub art. 9 Dekretu (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) albo art. 13 lub art. 14 RODO, oraz wskazuje przysługujące im uprawnienia, takie jak:

1) prawo do informacji o przetwarzaniu danych,
2) prawo do żądania sprostowania danych,
3) prawo do żądania dokonania adnotacji i uzupełnienia danych,
4) prawo do żądania usunięcia danych (prawo do bycia zapomnianym),
5) prawo do żądania ograniczenia przetwarzania,
6) prawo do cofnięcia zgody na przetwarzanie danych (bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem),
7) prawo do wniesienia skargi do organu nadzorczego.

3. ADO zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających, realizujących obowiązki wynikające z Dekretu albo RODO. W razie wystąpienia incydentu technicznego lub fizycznego zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

4. Potwierdzenie spełniania obowiązków informacyjnych przez ADO stanowią klauzule informacyjne przekazywane osobom, których dane osobowe są przetwarzane. Klauzule informacyjne są również wywieszane w widocznym miejscu w siedzibie WŻCh w Warszawie oraz na stronie internetowej ADO.

§ 3.
Upoważnienia do przetwarzania danych osobowych

1. ADO zapewnia, aby dostęp do danych osobowych w WŻCh miały tylko osoby legitymujące się nadanym upoważnieniem.
2. ADO udziela upoważnienia stałego Koordynatorom Lokalnym (KL) do udzielania dalszych upoważnień do przetwarzania danych osobowych, w szczególności koordynatorom rekolekcji w życiu codziennym.
3. Upoważnienia nadane przez ADO lub KL określają, do jakich czynności przetwarzania danych osobowych użytkownicy są uprawnieni (w szczególności do: tworzenia, usuwania, wglądu, przekazywania danych) oraz w jakich systemach informatycznych i na jaki czas.
4. ADO zapewnia prowadzenie przez IOD *Ewidencji osób upoważnionych do przetwarzania danych.*

§ 4.
Analiza ryzyka

ADO prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie nie rzadziej niż raz na dwa lata.

§ 5.
Wykaz zabezpieczeń

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

§ 6.
Rejestr czynności przetwarzania

ADO zapewnia prowadzenie przez IOD *Rejestru czynności przetwarzania danych osobowych*. W Rejestrze tym zamieszcza się:

1) nazwę oraz dane kontaktowe ADO,
2) nazwę oraz dane kontaktowe IOD,
3) cele przetwarzania,
4) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
5) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
6) gdy ma to zastosowanie, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku takiego transferu – dokumentację odpowiednich zabezpieczeń,
7) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
8) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

§ 7.
Procedura postępowania z incydentami

1. ADO wdraża procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 27 Dekretu albo art. 33 i art. 34 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych.

2. Powiadomienia wymagają:

1) udostępnienie danych osobowych osobom nieupoważnionym,
2) niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
3) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
4) nieprzestrzeganie zasad ochrony danych osobowych przez użytkowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
5) zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
6) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
7) nieuprawniona obecność osób postronnych w pomieszczeniach, gdzie przetwarzane są dane,

8) złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
9) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz pomieszczeń, gdzie przechowywane są dane osobowe, bez zezwolenia ADO,
10) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
11) awarie serwera, komputerów, twardych dysków, oprogramowania, zainfekowanie komputerów wirusem lub inne błędne działania komputerów,
12) telefoniczne próby wyłudzenia danych osobowych,
13) maile nakłaniające do ujawnienia identyfikatora lub hasła,
14) włamanie do systemu informatycznego lub pomieszczeń, gdzie przechowuje się dane osobowe, kradzież danych/sprzętu, zagubienie komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
15) świadome zniszczenie dokumentów w postaci papierowej lub elektronicznej.

3. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek niezwłocznego poinformowania IOD i jednocześnie właściwego KL o możliwości wystąpienia incydentu lub o jego wystąpieniu.

4. IOD lub KL zobowiązani są udokumentować wystąpienie incydentu i jego skutki oraz podjąć odpowiednie działania naprawcze i zaradcze.

5. KL niezwłocznie (nie później niż w ciągu 24 godzin) informuje IOD o wystąpieniu incydentu oraz o jego skutkach.

6. W razie potwierdzenia okoliczności, o których mowa w ust. 5, IOD zgłasza naruszenie ochrony danych osobowych Kościelnemu Inspektorowi Ochrony Danych (KIOD) albo Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), nie później niż 72 godziny po stwierdzeniu naruszenia oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

§ 8.
Regulamin ochrony danych osobowych i szkolenia wewnętrzne

1. ADO wprowadza w WŻCh, *Regulamin ochrony danych osobowych (wraz z załącznikami nr 1 i 2, tj. Polityką czystego biurka, Polityką kluczy)*, zwany dalej „Regulaminem", w celu zapewnienia osobom przetwarzającym dane osobowe pełny zakres wiedzy na temat zasad przetwarzania danych osobowych w WŻCh oraz obowiązków z tym związanych.

2. Osoby zapoznane z Regulaminem zobowiązane są potwierdzić fakt zapoznania się z tym dokumentem oraz zadeklarować stosowanie się do jego zasad. W przypadku braku rzeczywistych możliwości potwierdzenia podpisem faktu zapoznania się Regulaminem oraz klauzulą informacyjną dopuszcza się potwierdzenie tego faktu przez osobę upoważnioną.

3. Każda osoba przed powierzeniem jej przetwarzania danych osobowych powinna zostać zapoznana z Regulaminem.

4. ADO zapewnia przeszkolenie użytkowników z zakresu stosowania przepisów dotyczących ochrony danych osobowych, a ich obecność na szkoleniu należy potwierdzić pisemnie.

§ 9.
Umowy powierzania przetwarzania danych osobowych

1. W przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym ADO zobowiązany jest zawrzeć umowę powierzenia. Powierzenie przetwarzania danych podmiotowi nienależącemu do porządku kanonicznego musi zostać dokonane na podstawie umowy zawartej zgodnie z kan. 1290 Kodeksu Prawa Kanonicznego, z zastrzeżeniem, że także na podmiocie, któremu zostają powierzone dane, spoczywa obowiązek zachowania przepisów Dekretu albo zgodnie z art. 28 RODO.

2. Umowa powierzenia określa kategorie osób, których dane dotyczą, oraz obowiązki i prawa ADO. Ponadto, zobowiązuje podmiot przetwarzający do:

1) przetwarzania danych wyłącznie w zakresie i celu określonym w umowie;
2) zapewnienia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy;
3) podejmowania środków wymaganych w celu zabezpieczenia danych;
4) pomagania ADO wypełniać obowiązki w zakresie informowania osób, których dane dotyczą, realizowania ich uprawnień oraz obowiązków dotyczących zawiadamiania o naruszeniach;
5) po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji ADO, usunięcia lub zwrócenia mu wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii;
6) udostępniania ADO wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwianie ADO przeprowadzanie audytów.

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

4. W WŻCh prowadzony jest ***Rejestr umów powierzenia przetwarzania danych osobowych***.

§ 10.
Czynności kontrolne

1. Nadzór i kontrolę nad ochroną danych osobowych w WŻCh sprawuje prezydent WŻCh.

2. Czynności kontrolne przeprowadzane są cyklicznie nie rzadziej niż raz na dwa lata oraz doraźnie, gdy zaistnieje taka potrzeba. Czynności kontrolne mogą zostać przeprowadzone na zlecenie prezydenta WŻCh.

3. Z czynności kontrolnych sporządza się protokół, w którym dokonuje się opisu zakresu kontroli i przeprowadzonych czynności, a także zaleceń i działań naprawczych. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne.

§ 11.
Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Osoby upoważnione do przetwarzania danych osobowych ponoszą odpowiedzialność za niezastosowanie się do prowadzonej przez ADO polityki bezpieczeństwa danych osobowych, której założenia określa niniejszy dokument, na zasadach określonych w odrębnych przepisach.

Warszawa, dnia 26.02.2024

Marta Leonarda Hawrianna

Marcin Telich
.....
(podpis/-sy)

Załączniki:

- Regulamin ochrony danych osobowych – załącznik nr 1
- Polityka czystego biurka – załącznik nr 2
- Polityka kluczy – załącznik nr 3