KONFERENCJA EPISKOPATU POLSKI

KOŚCIELNY INSPEKTOR OCHRONY DANYCH

Praktyczne wskazania

z dnia 8 maja 2026 r.

dotyczące podmiotów kościelnych działających w obszarze pomocy społecznej

Opracowane przez KIOD
we współpracy z Prezesem Urzędu Ochrony Danych Osobowych

URZĄD OCHRONY DANYCH OSOBOWYCH

https://kiod.episkopat.pl/

SPIS TREŚCI

SKRÓTY:

- RODO – rozporządzenie 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.U.UE.L.2016.119.1 i Dz.U.UE.L.2018.127.2).
- Dekret – Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski, w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r., „Akta Konferencji Episkopatu Polski" 2018 nr 30, s. 31–54.
- EOG – Europejski Obszar Gospodarczy (27 państw UE oraz: Islandia, Liechtenstein i Norwegia).

ZASTRZEŻENIA:

a) Niniejsze praktyczne wskazania należy traktować jako wykonywanie przez Kościelnego Inspektora9 Ochrony Danych (KIOD) zadań, o których mowa w art. 37 ust. 1 pkt 2 i 3 Dekretu ogólnego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim („Dekret"), tj. upowszechnianie wiedzy o ochronie danych osobowych w Kościele oraz doradzanie administratorom danych.

b) Dokument niniejszy stanowi połączenie wymogów RODO, standardów określonych w Dekrecie oraz wniosków płynących z praktyki nadzorczej Kościelnego Inspektora Ochrony Danych oraz Prezesa Urzędu Ochrony Danych Osobowych.

c) Niniejsze praktyczne wskazania są przeznaczone wyłącznie do użytku wewnętrznego podmiotów kościelnych, w szczególności kościelnych publicznych osób prawnych prowadzących domy pomocy społecznej (DPS).

d) Wzory dokumentów (klauzule informacyjne, upoważnienia, elementy umowy powierzenia) zostały zamieszczone w odrębnym rozdziale na końcu dokumentu i mają charakter pomocniczy – wymagają każdorazowego dostosowania do specyfiki konkretnego domu pomocy społecznej.

e) Zastosowanie się do niniejszych praktycznych wskazań, przed ich zmianą, wyłącza odpowiedzialność jedynie względem KIOD, nie wyłącza natomiast odpowiedzialności przewidzianej w prawie kanonicznym, w tym w Dekrecie, RODO ani prawie powszechnie obowiązującym.

f) Niniejsze praktyczne wskazania powinny być stosowane *mutatis mutandis* przez kościelne podmioty prowadzące działalność w obszarze pomocy społecznej, z uwzględnieniem specyfiki danej placówki, pamiętając o zasadzie pierwszeństwa ochrony godności i prywatności osoby ludzkiej, wynikającej zarówno z nauczania Kościoła katolickiego, prawa kanonicznego, a szczególnie kan. 220 Kodeksu Prawa Kanonicznego i Dekretu oraz prawa powszechnie obowiązującego, w tym także z RODO.

1. WSTĘP

Kościelne domy pomocy społecznej (dalej: „DPS") prowadzone przez publiczne kościelne osoby prawne działają zazwyczaj w sferze tzw. spraw mieszanych: realizują jednocześnie cele kościelne (dzieła miłosierdzia) oraz zadania wynikające z prawa państwowego, w szczególności z ustawy o pomocy społecznej i umów zawieranych z jednostkami samorządu terytorialnego.

W konsekwencji przetwarzanie danych osobowych w DPS podlega równocześnie:

a) przepisom RODO (w szczególności art. 5–7, 9, 12–15, 24, 28–32, 30, 33–35),

b) przepisom Dekretu, który w wielu miejscach **odpowiada** regulacjom RODO:

- **art. 6 Dekretu** – zasady przetwarzania (odpowiednik art. 5 RODO),
- **art. 7 Dekretu** – przesłanki dopuszczalności przetwarzania (odpowiednik art. 6 i 9 RODO),
- **art. 8–9 Dekretu** – obowiązek informacyjny (odpowiednik art. 13–14 RODO),
- **art. 11–16 Dekretu** – prawa osób, których dane dotyczą (odpowiednik art. 15–18, 20–21 RODO),
- **art. 17, 22 Dekretu** – obowiązek wdrożenia środków technicznych i organizacyjnych (odpowiednik art. 24, 25, 32 RODO),
- **art. 19–21 Dekretu** – powierzenie przetwarzania, upoważnienia, rejestr czynności (odpowiednik art. 28–30, 29, 32 ust. 4 RODO),
- **art. 27–28 Dekretu** – naruszenia ochrony danych (odpowiednik art. 33–34 RODO),
- **art. 30–32 Dekretu** – inspektor ochrony danych (odpowiednik art. 37–39 RODO).

W codziennej praktyce DPS powinien więc zakładać **nakładające się reżimy ochronne**: to, co jest wymagane przez RODO, ma – co do zasady – swój odpowiednik w Dekrecie i powinno być spełnione „podwójnie", z uwzględnieniem właściwego organu (PUODO / KIOD) i właściwego porządku prawnego (świecki / kanoniczny).

1.1. Status administratora danych – DPS jako administrator

a) Zgodnie ze stanowiskiem przyjętym w praktyce organów nadzorczych i znajdującym potwierdzenie w decyzjach Prezesa Urzędu Ochrony Danych Osobowych, **administratorem danych jest Dom Pomocy Społecznej** jako wyodrębniona jednostka organizacyjna zgromadzenia zakonnego lub innej kościelnej osoby prawnej, o ile to DPS faktycznie ustala cele i sposoby

przetwarzania danych osobowych w związku z realizacją zadania publicznego i działalności pomocowej.

b) Zgromadzenie zakonne (lub inna kościelna publiczna osoba prawna prowadząca DPS) pozostaje podmiotem nadrzędnym w strukturze kościelnej i organizacyjnej. W zakresie, w jakim nie wyznacza samodzielnie celów i sposobów przetwarzania danych w ramach DPS, nie jest odrębnym administratorem, lecz podmiotem sprawującym nadzór organizacyjny, prawny i kościelny.

c) W dokumentach wewnętrznych ochrony danych oraz w klauzulach informacyjnych DPS, a także w innych dokumentach (akty erekcyjne, statuty, regulaminy organizacyjne, zarządzenia wewnętrzne) należy **jednoznacznie i konsekwentnie wskazywać tę samą jednostkę jako administratora** danych osobowych (np. „Administratorem Pani/Pana danych osobowych jest Dom Pomocy Społecznej Zgromadzenia … w … z siedzibą w …"), unikając wprowadzania w błąd co do kompetencji DPS i zgromadzenia oraz niepoprawnego podawania jako administratora przetwarzanych danych osobowych np. dyrektora DPS.

d) Dyrektor DPS pełni funkcję osoby reprezentującej administratora (jest on organem administratora). W rzadkich przypadkach Dyrektor DPS może stać się odrębnym, samodzielnym administratorem, jeżeli na to wskazuje stan faktyczny lub prawny.

e) W przypadku wspólnych operacji przetwarzania danych z innymi podmiotami (np. powiat, inna placówka pomocy społecznej, inna jednostka organizacyjna zgromadzenia) należy rozważyć zastosowanie konstrukcji **współadministratorów** (art. 26 RODO; w Dekrecie – art. 18) i odpowiednio opisać w wewnętrznym uzgodnieniu podział obowiązków i praw, udostępniając informację o tym podziale osobom, których dane dotyczą.

1.2. Dane przetwarzane w kościelnym DPS

W kościelnym DPS przetwarzane są w szczególności:

a) **Dane mieszkańców** – dane zwykłe (np. imię i nazwisko, dane z monitoringu, sytuacji rodzinnej, dane o świadczeniach socjalnych) oraz dane należące do szczególnych kategorii (np. dane dotyczące zdrowia, niepełnosprawności, opinie psychologiczne, psychiatryczne, orzeczenia o stopniu niepełnosprawności).

- RODO: art. 9 ust. 1–2, art. 6 ust. 1
- Dekret: art. 7 ust. 1–2

c) **Dane członków rodzin i opiekunów prawnych** dane zwykłe (np. dane kontaktowe, sytuacja materialna, dane identyfikacyjne) oraz dane szczególne (np. dane dotyczące zdrowia podane w związku ze sprawą związaną z wykonywaniem swoich obowiązków wobec mieszkańca).
    - RODO: art. 9 ust. 1–2, art. 6 ust. 1
    - Dekret: art. 7 ust. 1–2

d) **Dane pracowników i współpracowników DPS** (np. dane kadrowe wymagane art. 22(1) k.p., dane o zdrowiu – np. badania okresowe, dane o wynagrodzeniu, dane osób kontaktowych w sytuacjach awaryjnych; w przypadku DPS dla osób małoletnich – dane osób dopuszczonych do pracy z tymi osobami konieczne do wykonania obowiązku weryfikacji zgodnie z ustawą z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich.
    - RODO: art. 6 ust. 1 lit. b, c, f; art. 9 ust. 2 lit. b, h, art. 10 (w DPS dla osób małoletnich)
    - Dekret: art. 7 ust. 1 pkt 2–3 i 6; art. 7 ust. 2

e) **Dane kontrahentów, darczyńców, wolontariuszy** (np. imię i nazwisko, numer rachunku bankowego, NIP, nr PESEL).
    - RODO: art. 6 ust. 1 lit. b, c, f
    - Dekret: art. 7 ust. 1 pkt 2–3 i 6, art. 7 ust. 2

f) **Dane użytkowników strony internetowej DPS oraz fanpage na portalach społecznościowych** (np. adresy IP, identyfikatory plików cookies).
    - RODO: art. 6 ust. 1 lit. f
    - Dekret: art. 7 ust. 1 pkt 6

g) **Dane osób kontaktujących się z DPS,** np. w celu uzyskania informacji.
    - RODO: art. 6 ust. 1 lit. f
    - Dekret: art. 7 ust. 1 pkt 6

Wszystkie te dane muszą być przetwarzane zgodnie z zasadami określonymi w art. 5 RODO oraz w art. 6 Dekretu (zgodność z prawem, rzetelność i przejrzystość; ograniczenie celu; minimalizacja danych; prawidłowość; ograniczenie przechowywania; integralność i poufność; rozliczalność – por. art. 5 ust. 2 RODO oraz art. 6 ust. 2 Dekretu).

1.3. Podstawy prawne przetwarzania

1.3.1. Mieszkańcy DPS

Podstawami przetwarzania danych mieszkańców są w szczególności:

a) **obowiązek prawny administratora** – art. 6 ust. 1 lit. c RODO w zw. z przepisami ustaw o pomocy społecznej, o ochronie zdrowia psychicznego, o działalności leczniczej itp.; w Dekrecie – art. 7 ust. 1 pkt 3 (wypełnienie obowiązku prawnego ciążącego na administratorze, określonego w przepisach prawa kanonicznego lub prawa powszechnie obowiązującego),

b) **wykonywanie zadania realizowanego w interesie publicznym** – art. 6 ust. 1 lit. e RODO w zw. z odpowiednimi przepisami sektorowymi (w Dekrecie – art. 7 ust. 1 pkt 5),

c) **dla szczególnych kategorii danych** – art. 9 ust. 2 lit. b, h RODO (opieka zdrowotna, zabezpieczenie społeczne); w Dekrecie – art. 7 ust. 2 (dane wrażliwe), w związku z celami kościelnymi określonymi w Kodeksie Prawa Kanonicznego i przepisami wewnętrznymi zgromadzenia (opieka nad chorymi, działalność charytatywna),

d) **zgoda** (art. 6 ust. 1 lit. a RODO; art. 7 ust. 1 pkt 1 Dekretu) powinna być stosowana **wyjątkowo**, głównie dla celów dodatkowych (np. publikacja wizerunku mieszkańca na stronie DPS, materiały promocyjne, uczestnictwo w wydarzeniach niezwiązanych bezpośrednio ze statutową działalnością DPS).

UWAGA: Cel informacyjny lub promocyjny DPS można osiągnąć bez przetwarzania danych osobowych mieszkańców; należy szczególnie z rozwagą i dbałością o uszanowanie prywatności podchodzić do publikacji wizerunków tych osób na stronie internetowej lub w portalach społecznościowych.

1.3.2. Pracownicy i kandydaci do pracy oraz personel wykonujący zadania na innej podstawie prawnej niż umowa o pracę

a) Dane niezbędne do zawarcia i wykonania umowy o pracę lub na podstawie stosunku cywilnoprawnego – art. 6 ust. 1 lit. b RODO, w Dekrecie – art. 7 ust. 1 pkt 2.

b) Dane przetwarzane w celu realizacji obowiązków wynikających z prawa pracy, BHP – art. 6 ust. 1 lit. c RODO; w Dekrecie – art. 7 ust. 1 pkt 3.

c) W uzasadnionych przypadkach – prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO; art. 7 ust. 1 pkt 6 Dekretu), np. w zakresie dochodzenia roszczeń, jeżeli ze specyfiki relacji administrator–osoba fizyczna można racjonalnie przyjąć, że przetwarzanie danych jest

niezbędne do zrealizowania przez administratora celu wynikającego z tej relacji, chyba że interesy lub podstawowe prawa i wolności osoby, której przetwarzane dane dotyczą, będą nadrzędne wobec interesu administratora.

UWAGA: Niedopuszczalne jest przetwarzanie danych osobowych na zapas z abstrakcyjnym założeniem, że mogą być one ewentualnie przydatne w przyszłości.

d) Dane przetwarzane na podstawie zgody pracownika (art. 6 ust. 1 lit. a RODO i art. 7 ust. 1 pkt 1 Dekretu – w zakresie np. adresu e-mail, nr prywatnego telefonu, wizerunku (pozyskanego w inny sposób niż monitoring wizyjny).

e) Dla **szczególnych kategorii danych** – art. 9 ust. 2 lit. b RODO (prawo pracy, zabezpieczenie społeczne i ochrona socjalna); w Dekrecie – art. 7 ust. 2 (dane wrażliwe), w związku z celami kościelnymi określonymi w Kodeksie Prawa Kanonicznego i przepisami wewnętrznymi zgromadzenia.

1.3.3. Kontrahenci, darczyńcy, wolontariusze

a) **prawnie uzasadniony interes administratora** (art. 6 ust. 1 lit. f RODO; art. 7 ust. 1 pkt 6 Dekretu),

b) **wykonanie umowy** (art. 6 ust. 1 lit. b RODO; art. 7 ust. 1 pkt 2 Dekretu), (np. umowy wolontariackiej, umowy darowizny),

c) **zgoda** (art. 6 ust. 1 lit. a RODO; art. 7 ust. 1 pkt 1 Dekretu) powinna być stosowana **wyjątkowo**, głównie dla celów dodatkowych (np. publikacja wizerunku, materiały promocyjne, udział w zajęciach dodatkowych).

1.4. Administrator, podmiot przetwarzający, odbiorcy

a) **Administratorem** jest – jak wskazano w pkt 1.1 – Dom Pomocy Społecznej (DPS) jako jednostka organizacyjna kościelnej publicznej osoby prawnej, która **ustala cele i sposoby przetwarzania danych**.

- RODO: definicja z art. 4 pkt 7, obowiązki m.in. z art. 24, 25
- Dekret: definicja art. 5 pkt 4, obowiązki m.in. z art. 17

b) **Podmiot przetwarzający** to np. firma obsługująca systemy informatyczne, zewnętrzna księgowość, firma serwisująca oprogramowanie medyczne, firmy archiwizujące dokumenty, podmioty niszczące dokumenty.
   - RODO: art. 4 pkt 8, art. 28
   - Dekret: art. 5 pkt 5, art. 19

   Wybór i nadzór nad podmiotami przetwarzającymi powinien odpowiadać wymaganiom art. 28 RODO i art. 19 Dekretu (umowa powierzenia z wyraźnym określeniem obowiązków, zakresu danych, kategorii osób, obowiązku poufności, usunięcia lub zwrotu danych po zakończeniu współpracy, prawa audytu).

c) **Odbiorcami danych** są podmioty, którym dane są ujawniane (np. starostwo, NFZ, lekarze kontraktowi, inne instytucje pomocy społecznej, sądy i organy ścigania, usługodawcy zewnętrzni prowadzący zajęcia mieszkańców).
   - RODO: art. 4 pkt 9
   - Dekret: art. 5 pkt 6

   Z zastrzeżeniem, że odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem.

DPS ma obowiązek **jasnego i szczegółowego wskazywania odbiorców lub kategorii odbiorców** zarówno w klauzulach informacyjnych (art. 13 ust. 1 lit. e i art. 14 ust. 1 lit. e RODO; art. 8–9 Dekretu), jak i w rejestrze czynności przetwarzania (art. 30 ust. 1 lit. d RODO; art. 21 Dekretu). Podawanie ogólnej informacji typu „organy administracji publicznej" bez konkretyzacji stanowi naruszenie zasady przejrzystości i obowiązku informacyjnego.

1.5. Środki techniczne i organizacyjne, analiza ryzyka

RODO zobowiązuje administratora do szeregu obowiązków wskazanych w rozdziale IV (analogiczny rozdział IV Dekretu) w tym do wdrożenia „odpowiednich środków technicznych i organizacyjnych".

W DPS oznacza to m.in.:

a) przeprowadzenie **analizy ryzyka** (najlepiej utrwalonej w formie dokumentu) dla głównych operacji przetwarzania danych,
b) przypisanie środków bezpieczeństwa (organizacyjnych, technicznych, fizycznych) do zidentyfikowanych ryzyk,

c) dokumentowanie tych działań i ich okresowe przeglądy (art. 24 ust. 1–2 RODO; art. 17 ust. 1–3 i art. 22 Dekretu),

d) zgodnie z decyzjami PUODO, DPS ma obowiązek wdrożenia **procedur testowania, mierzenia i oceniania skuteczności środków bezpieczeństwa** (art. 24 ust. 2 w zw. z art. 32 ust. 1 lit. d RODO). Brak takich procedur jest uznawany za naruszenie tych przepisów.

1.6. Rejestr czynności, dokumentacja

Administrator prowadzi **rejestr czynności przetwarzania** zgodnie z art. 30 RODO. Dekret przewiduje analogiczny obowiązek w art. 21 (zakres informacji bardzo zbliżony: cele, kategorie osób i danych, odbiorcy, planowane terminy usunięcia, ogólny opis środków bezpieczeństwa).

Przedmiotowy rejestr w DPS powinien obejmować m.in.:

a) przyjęcie mieszkańca oraz prowadzenie dokumentacji jego pobytu i opieki nad nim,

b) prowadzenie dokumentacji medycznej (jeżeli DPS ją wytwarza, np. stosuje się w nim przymus bezpośredni – art. 18b ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego lub ogranicza możliwości samodzielnego opuszczania terenu DPS przez mieszkańca – art. 55 ust. 2b ustawy z dnia 12 marca 2004 r. o pomocy społecznej),

c) zatrudnianie pracowników i obsługę kadrowo-płacową,

d) obsługę wolontariuszy,

e) obsługę darczyńców,

f) prowadzenie monitoringu wizyjnego (jeżeli jest),

g) obsługę stron internetowych, kampanii informacyjnych,

h) kontakt z rodzinami,

i) rejestr zdarzeń nadzwyczajnych.

W każdej z powyższych czynności DPS powinien – zgodnie z decyzjami PUODO – **konkretnie wskazać odbiorców lub kategorie odbiorców** (art. 30 ust. 1 lit. d RODO) oraz **określić planowane terminy usunięcia danych** w sposób precyzyjny, a nie ogólnikowy (np. „10 lat od zakończenia zatrudnienia" zamiast „zgodnie z przepisami").

1.7. Prawa osób, których dane dotyczą

RODO (art. 12–15, 16–18, 20–21, 22) i Dekret (art. 11–16) przewidują analogiczny katalog praw: prawo dostępu, sprostowania, uzupełnienia, usunięcia (z zastrzeżeniami), ograniczenia przetwarzania,

sprzeciwu wobec przetwarzania, informacji o odbiorcach, prawo do skargi do niezależnego organu nadzorczego (PUODO / KIOD).

DPS powinien mieć **spójną procedurę obsługi wniosków**:

a) identyfikacja osoby,
b) weryfikacja zakresu prawa (czy zachodzą wyjątki, np. dokumentacja archiwalna, obowiązki prawne),
c) terminowe udzielenie odpowiedzi (RODO: co do zasady 1 miesiąc – art. 12 ust. 3; Dekret: odpowiednie przepisy proceduralne przy prawach osób, których dane dotyczą „bez zbędnej zwłoki", niezwłocznie" lub 3 miesiące *per analogiam* do kan. 57 § 1),
d) dokumentowanie w rejestrze wniosków.

2. PRAKTYCZNE WSKAZANIA DLA KOŚCIELNYCH DPS

2.1. Identyfikacja administratora i zakresu odpowiedzialności

a) W akcie erekcyjnym DPS, regulaminie organizacyjnym lub innym dokumencie wewnętrznym należy **jednoznacznie wskazać, kto jest administratorem** w rozumieniu art. 4 pkt 7 RODO oraz art. 5 pkt 4 Dekretu (np. „Administratorem Państwa danych osobowych jest Dom Pomocy Społecznej Zgromadzenia X w Y, wyodrębniona jednostka organizacyjna [nazwa kościelnej osoby prawnej]").

b) Należy unikać niejednoznacznych lub błędnych sformułowań typu: raz DPS, raz dyrektor DPS jako administrator. Dyrektor pełni funkcję osoby reprezentującej administratora, lecz nie staje się odrębnym administratorem, o ile tak nie postanowiono wyraźnie w konkretnym akcie prawnym.

c) W przypadku wspólnych operacji z innymi podmiotami (np. powiat, inna placówka, fundacja, stowarzyszenie) należy rozważyć zastosowanie konstrukcji **współadministratorów** (art. 26 RODO; w Dekrecie – art. 18) i odpowiednio opisać podział obowiązków.

d) W umowach z kontrahentami, podmiotami przetwarzającymi oraz w korespondencji z organami państwowymi DPS powinien konsekwentnie występować jako administrator, zapewniając przejrzystość i jednoznaczność statusu prawnego.

e) Należy koniecznie ujednolicić nazwę podmiotu w dokumentach, pieczątkach, rejestrach, itd.

2.2. Analiza ryzyka i środki bezpieczeństwa

a) Przeprowadzić **formalną analizę ryzyka** dla wszystkich kluczowych czynności przetwarzania, uwzględniając:

- dane szczególnych kategorii (art. 9 RODO; art. 7 ust. 2 Dekretu),
- osoby wymagające szczególnej uwagi (np. osoby niepełnosprawne intelektualnie, chorzy psychicznie),
- różne nośniki i miejsca przetwarzania danych (papierowe i elektroniczne),
- dane udostępniane na portalach społecznościowych (administrator, oceniając procesy przetwarzania danych osobowych i przekazując informacje za pośrednictwem serwisów będących własnością innych administratorów, musi pamiętać o konieczności dokonania

oceny związanych z tym ryzyk, a przede wszystkim oceny ról podmiotów występujących w tych procesach),

- w przypadku DPS dla osób małoletnich – obowiązkowa weryfikacja danych osób dopuszczonych do pracy z małoletnimi zgodnie z ustawą z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich.

b) Na podstawie analizy wdrożyć środki zgodnie z art. 32 RODO i art. 22 Dekretu, w szczególności:

- kontrolę dostępu (role, hasła, uprawnienia w systemach),
- zabezpieczenia fizyczne (szafy zamykane, kontrola kluczy, ograniczony dostęp do pomieszczeń z dokumentacją i serwerowni),
- szyfrowanie nośników przenośnych, ochrona antywirusowa, kopie zapasowe,
- procedury postępowania z dokumentacją papierową (obieg, archiwizacja, niszczenie).

c) Analizę i dobór środków należy **udokumentować** i okresowo przeglądać (art. 24 ust. 1–2 RODO; art. 17 ust. 1-2 Dekretu).

d) **Wdrożyć procedury testowania skuteczności środków** – zgodnie z decyzjami PUODO brak takich procedur stanowi naruszenie art. 24 ust. 2 i art. 32 ust. 1 lit. d RODO. DPS powinien:

- przyjąć pisemną procedurę dokonywania okresowych przeglądów środków bezpieczeństwa,
- określić harmonogram przeglądów (np. raz w roku, częściej przy zmianach organizacyjnych, po incydencie mającym wpływ na przyjęte rozwiązania),
- wyznaczyć osoby odpowiedzialne za konkretne czynności (np. IOD – doradza i monitoruje, dyrektor DPS – podejmowanie decyzji),
- dokumentować przeglądy i działania naprawcze w dedykowanym rejestrze.

2.3. Polityka ochrony danych i procedury wewnętrzne

a) Na podstawie art. 24 ust. 2 RODO i art. 17 ust. 2 Dekretu zaleca się przyjęcie jednej, spójnej **polityki ochrony danych osobowych w DPS**, obejmującej:

- opis ról i odpowiedzialności (np. Dyrektor, IOD, osoby upoważnione),
- zasady nadawania i cofania upoważnień (art. 29 i 32 ust. 4 RODO; art. 20 i 22 ust. 3 Dekretu),

- procedurę obsługi naruszeń (art. 33–34 RODO; art. 27–28 Dekretu),
- procedurę realizacji praw osób, których dane dotyczą,
- zasady współpracy z podmiotami przetwarzającymi (art. 28 RODO; art. 19 Dekretu),
- zasady prowadzenia rejestru czynności (art. 30 RODO; art. 21 Dekretu),
- zasady szkoleń i podnoszenia świadomości personelu,
- procedurę testowania i przeglądów środków bezpieczeństwa (odniesienie do art. 32 ust. 1 lit. d RODO).

b) Polityka powinna być **formalnie przyjęta** (zarządzenie administratora, data wejścia w życie, numer wersji), udostępniona wszystkim osobom przetwarzającym dane i wdrożona.

c) **Wdrożenie polityki wymaga**:

- formalnego zatwierdzenia przez osobę uprawnioną do reprezentowania DPS (np. zarządzenie wewnętrzne z datą, numerem i podpisem Dyrektora DPS),
- pisemnego potwierdzenia zapoznania się z polityką przez wszystkich pracowników i osoby współpracujące (lista podpisów lub oświadczenia indywidualne) oraz zobowiązania się przez te osoby do jej przestrzegania,
- udokumentowanego przekazania polityki nowym pracownikom (wpis w karcie szkolenia wstępnego lub odrębne oświadczenie),
- przechowywania dokumentacji potwierdzającej wdrożenie w sposób umożliwiający wykazanie rozliczalności przed organem nadzorczym.

d) Brak udokumentowania wdrożenia polityki, nawet przy jej faktycznym istnieniu, stanowi naruszenie art. 24 ust. 2 RODO i art. 5 ust. 2 RODO (zasada rozliczalności) oraz art. 17 ust. 2 i art. 6 ust. 2 Dekretu (zasada rozliczalności). Sam fakt podpisania polityki przez Dyrektora nie jest wystarczający – konieczne jest również wykazanie, że została ona rzeczywiście wprowadzona do stosowania i zapoznali się z nią wszyscy pracownicy przetwarzający dane, jak również zobowiązali się do jej przestrzegania.

e) Polityka powinna być okresowo przeglądana i aktualizowana (co najmniej raz w roku oraz przy istotnych zmianach organizacyjnych, prawnych lub technicznych), a także w razie zaistnienia incydentu wskazującego na konieczność udoskonalenia przyjętych w polityce rozwiązań.

2.4. Obowiązek informacyjny

2.4.1. Wymagania ogólne

a) Dla każdej głównej kategorii osób należy przygotować **oddzielne, przejrzyste klauzule informacyjne**:

- mieszkańcy i ich opiekunowie,
- osoby odwiedzające,
- pracownicy i kandydaci do pracy, personel wykonujący zadania na innej podstawie prawnej niż umowa o pracę,
- darczyńcy,
- kontrahenci,
- wolontariusze.

b) Klauzule muszą spełniać wymagania art. 13–14 RODO i odpowiednio art. 8–9 Dekretu, tj. zawierać m.in.:

- dane administratora i kontakt do IOD, jeżeli został powołany,
- cele i podstawy prawne przetwarzania z jasnym powiązaniem (np. „prowadzenie domu pomocy społecznej dla osób niepełnosprawnych intelektualnie – art. 6 ust. 1 lit. e RODO w zw. z ustawą o pomocy społecznej oraz art. 7 ust. 1 pkt 5 Dekretu").

UWAGA: Podstawa określona w lit. e zależy od tego, czy DPS ma podpisaną umowę z jednostką samorządu terytorialnego.

- prawnie uzasadniony interes realizowany przez administratora (gdy ma to zastosowanie),
- kategorie odbiorców (np. organy administracji – lecz nie w ramach prowadzonych konkretnych postępowań – patrz pkt 1.4 lit c; firmy IT),
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, jeżeli ma to zastosowanie,
- planowane okresy przechowywania lub kryteria ich ustalenia (spójne z rejestrem czynności – art. 30 ust. 1 lit. f RODO; art. 21 ust. 1 pkt 6 Dekretu),
- informacje o prawach osób (RODO: art. 15–18, 20–21; Dekret: art. 11–16),
- jeżeli przetwarzania odbywa się na podstawie zgody – informację o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

- informację o prawie wniesienia skargi odpowiednio do PUODO i KIOD (art. 77 RODO; art. 41 Dekretu),
- informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych, gdy ma to zastosowanie,
- informację o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu (art. 22 RODO, art. 13 ust. 2 lit. f RODO; art. 3, por. art. 5 pkt 2 Dekretu), np. „Dane osobowe nie będą przetwarzane automatycznie (w tym poprzez profilowanie) w sposób wpływający na prawa osób".

2.4.2. Szczególne wymaganie: odbiorcy danych

a) Zgodnie z decyzjami PUODO klauzule informacyjne muszą zawierać **konkretną, szczegółową informację o odbiorcach** lub kategoriach odbiorców danych osobowych. Naruszenie tego obowiązku uznane zostało za naruszenie art. 5 ust. 1 lit. a (zasada przejrzystości), art. 12 ust. 1 oraz art. 13 ust. 1 lit. e i art. 14 ust. 1 lit. e RODO.

b) Wskazanie odbiorców powinno następować poprzez:

- **podanie pełnej nazwy i danych kontaktowych podmiotu**, któremu dane zostały ujawnione (np. „Starostwo Powiatowe w [nazwa], ul. [adres], NFZ Oddział Wojewódzki [nazwa], ul. [adres], Szpital Powiatowy w [nazwa], ul. [adres]),
- lub – gdy lista jest zmienna – poprzez **szczegółowe określenie kategorii odbiorców** (np. „organy administracji publicznej właściwe w sprawach pomocy społecznej na poziomie powiatu i województwa, Narodowy Fundusz Zdrowia, publiczne i niepubliczne zakłady opieki zdrowotnej realizujące świadczenia na rzecz mieszkańców, podmioty przetwarzające dane na podstawie umów powierzenia: firma [nazwa] świadcząca usługi informatyczne, firma [nazwa] prowadząca obsługę kadrowo-płacową").

c) W praktyce zaleca się stosowanie modelu mieszanego: podanie z nazwy kluczowych, stałych odbiorców oraz ogólnych kategorii dla odbiorców zmiennych, z możliwie największym stopniem szczegółowości. Przy długiej liście stałych odbiorców można podać tylko kategorię odbiorców i odesłać do konkretnego miejsca, gdzie znajduje się pełna lista.

2.4.3. Sposób przekazywania klauzul

a) W odniesieniu do danych pozyskiwanych z innych źródeł (np. dokumentacja przekazywana przez starostwo, szpital) należy wypełnić obowiązek informacyjny z art. 14 RODO oraz art. 9 Dekretu – co do zasady w rozsądnym terminie, nie później niż w ciągu miesiąca.

b) Klauzule dla mieszkańców powinny być:

- wręczane przy przyjęciu do DPS (wraz z dokumentacją przyjęcia),
- udostępnione w widocznych miejscach w budynku (np. przy recepcji, w gablocie informacyjnej),
- formułowane językiem prostym i zrozumiałym, z uwzględnieniem potrzeb osób z niepełnosprawnościami (art. 12 ust. 1 RODO).

c) Klauzule dla pracowników – wręczane przy zatrudnieniu, z potwierdzeniem zapoznania się, dostępne w stałym miejscu u pracodawcy np. w sekretariacie.

d) Dopuszczalne jest tzw. informowanie warstwowe – podstawowe informacje w skrótowej formie (np. administrator, IOD, cel i podstawa przetwarzania, prawa osób) + odesłanie do pełnej klauzuli dostępnej w konkretnym miejscu (np. strona WWW, gablotka).

2.4.4. Weryfikacja i aktualizacja klauzul informacyjnych

a) Przed wdrożeniem klauzuli informacyjnej DPS powinien przeprowadzić weryfikację formalną i merytoryczną:

- **Weryfikacja formalna**: czy klauzula zawiera wszystkie elementy wymagane art. 13–14 RODO oraz art. 8–9 Dekretu; czy informacje są spójne z rejestrem czynności przetwarzania; czy podstawy prawne są wskazane precyzyjnie i prawidłowo.
- **Weryfikacja merytoryczna**: czy we wszystkich klauzulach stosowanych przez DPS wskazano poprawnego (i tego samego) administratora (bez rozbieżności); czy język klauzuli jest prosty i zrozumiały dla adresata.
- **Weryfikacja spójności**: czy klauzula jest zgodna z polityką ochrony danych i faktyczną praktyką DPS.

b) **Typowe błędy do unikania (na podstawie praktyki orzeczniczej PUODO)**:

- Wskazywanie niepoprawne administratorów i inne ich określenie w różnych miejscach klauzuli (np. raz DPS, raz Dyrektor DPS) – naruszenie art. 13 ust. 1 lit. a RODO.

- Ogólnikowe wskazanie podstaw prawnych bez konkretnego powiązania z celem (np. „art. 6 ust. 1 lit. c RODO” bez wskazania, jaki konkretnie obowiązek prawny jest realizowany) – naruszenie art. 13 ust. 1 lit. c RODO.
- Brak precyzyjnego wskazania odbiorców lub kategorii odbiorców (np. „organy administracji publicznej” bez dalszej konkretyzacji) – naruszenie art. 13 ust. 1 lit. e RODO i zasady przejrzystości.
- Ogólnikowe wskazanie okresów przechowywania (np. „zgodnie z przepisami prawa”) – naruszenie art. 13 ust. 2 lit. a RODO.
- Nieprecyzyjne wskazanie praw osoby (np. „przysługuje prawo dostępu, sprostowania, usunięcia, ograniczenia przetwarzania, chyba że realizacja tych praw jest niezgodna z przepisami”) bez bliższego wyjaśnienia, w jakich przypadkach osoba może z tych praw skorzystać.

c) DPS powinien aktualizować klauzule informacyjne:

- przy każdej zmianie celów lub podstaw przetwarzania,
- przy zmianie odbiorców danych (np. zawarcie umowy z nowym podmiotem przetwarzającym),
- przy zmianie okresów przechowywania (np. zmiana przepisów dotyczących kwestii archiwalnych),
- przy zmianie danych kontaktowych administratora lub IOD.

d) Zaleca się przeprowadzanie systematycznego (np. corocznego) przeglądu wszystkich stosowanych klauzul informacyjnych (wraz z przeglądem polityki ochrony danych i rejestru czynności) w celu weryfikacji ich aktualności i zgodności z przepisami.

2.5. Umowy powierzenia przetwarzania

a) Z każdym podmiotem zewnętrznym, który **przetwarza dane w imieniu DPS** (np. firma IT, hostująca oprogramowanie, zewnętrzna księgowość, firma archiwizująca dokumenty, firma niszcząca dokumenty), należy zawrzeć pisemną umowę spełniającą wymogi:

- art. 28 RODO i art. 19 Dekretu (szczegółowe elementy umowy, gwarancje, zakres, obowiązek tajemnicy, usunięcie, zwrot danych, audyt).

UWAGA: Umowa powierzenia może stanowić odrębny dokument lub jej treść może być zawarta w postanowieniach umowy dotyczącej usługi (umowy głównej).

b) Umowa powinna w szczególności:

- określać rodzaj danych i kategorie osób,
- określać zakres i cel przetwarzania,
- wskazywać obowiązki i prawa administratora,
- przewidywać obowiązek poufności personelu podmiotu przetwarzającego,
- regulować warunki podpowierzenia innemu podmiotowi przetwarzającemu,
- określać sposób zakończenia przetwarzania (zwrot lub usunięcie danych oraz kopii).

c) DPS powinien wybrać podmioty przetwarzające, które dają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 28 ust. 1 RODO).

d) Przed zawarciem umowy zaleca się przeprowadzenie weryfikacji podmiotu przetwarzającego (referencje, dokumentacja, wcześniejsze audyty).

e) **Checklista weryfikacji umowy powierzenia przed jej podpisaniem**:

- Czy umowa zawiera pełne dane stron (nazwa, adres, NIP, przedstawiciele)?
- Czy określono przedmiot umowy (rodzaj usług)?
- Czy wskazano rodzaj danych osobowych (np. „dane identyfikacyjne i kontaktowe mieszkańców, dane dotyczące zdrowia")?
- Czy wskazano kategorie osób, których dane dotyczą (np. „mieszkańcy DPS, pracownicy DPS")?
- Czy wskazano charakter i cel przetwarzania?
- Czy określono czas trwania przetwarzania?
- Czy umowa zawiera wskazanie obowiązków i praw administratora?
- Czy umowa zawiera obowiązek przetwarzania wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO, art. 19 ust. 2 Dekretu)?
- Czy umowa zawiera obowiązek zachowania poufności przez osoby przetwarzające (art. 28 ust. 3 lit. b RODO, art. 19 ust. 2 pkt 2 Dekretu)?
- Czy umowa zawiera zobowiązanie do wdrożenia odpowiednich środków bezpieczeństwa (art. 28 ust. 3 lit. c RODO, art. 19 ust. 2 pkt 3 Dekretu)?
- Czy umowa reguluje kwestię dalszych podmiotów przetwarzających (art. 28 ust. 3 lit. d i ust. 2 RODO, art. 19 ust. 3 Dekretu)?
- Czy umowa zawiera zobowiązanie do pomocy administratorowi w realizacji obowiązków wobec osób, których dane dotyczą i z art. 32-36 RODO (art. 28 ust. 3 lit. e i f RODO,

art. 19 ust. 2 pkt 4 Dekretu) oraz na czym dokładnie ta pomoc ma polegać, a także w jakich terminach ma być realizowana?

- Czy umowa określa sposób zakończenia przetwarzania: zwrot lub usunięcie danych (art. 28 ust. 3 lit. g RODO, art. 19 ust. 2 pkt 5 Dekretu)?
- Czy umowa przewiduje prawo audytu administratora (art. 28 ust. 3 lit. h RODO, art. 19 ust. 2 pkt 6 Dekretu)?

f) W przypadku firm świadczących usługi informatyczne (hosting, serwisowanie systemów, kopie zapasowe) należy dodatkowo:

- uzyskać informację o lokalizacji serwerów (czy dane są przetwarzane w EOG),
- uzyskać informację o zastosowanych technicznych środkach bezpieczeństwa (szyfrowanie, kopie zapasowe, kontrola dostępu),
- uzgodnić procedurę postępowania w razie naruszenia ochrony danych po stronie procesora.

2.6. Upoważnienia i dostęp do danych

a) Na podstawie art. 29 RODO i art. 20 Dekretu DPS powinien zapewnić, aby osoby działające z upoważnienia administratora przetwarzały dane **wyłącznie w zakresie niezbędnym** do wykonywania swoich zadań.

b) W praktyce oznacza to:

- zdefiniowanie ról (np. pielęgniarka, opiekun, lekarz, kierownik, pracownik administracyjny, magazynier, pokojowa),
- przypisanie do każdej roli **konkretnego zakresu danych i operacji** (np. „pielęgniarka – dane medyczne mieszkańców swojego oddziału; obsługa dokumentacji lekowej; brak dostępu do danych kadrowych pracowników”),
- nadawanie upoważnień zawierających co najmniej: dane osoby, zakres danych, czynności i cel, datę nadania i cofnięcia, podpisy.

c) Należy prowadzić **rejestr upoważnień** oraz aktualizować uprawnienia przy każdej zmianie stanowiska lub zakresu obowiązków oraz sposobów przetwarzania.

d) Upoważnienia należy wydawać przed dopuszczeniem danej osoby do przetwarzania danych (*nie ex post*).

e) DPS powinien przeprowadzać regularne przeglądy upoważnień (co najmniej raz w roku oraz przy każdej istotnej zmianie organizacyjnej) w celu weryfikacji, czy:

- zakres upoważnienia odpowiada rzeczywistemu zakresowi przetwarzania danych przez daną osobę,
- nie występują rozbieżności między zakresem upoważnienia a faktycznymi obowiązkami służbowymi,
- upoważnienie nie jest zbyt szerokie (nadmierne uprawnienia) ani zbyt wąskie (uniemożliwiające wykonywanie zadań).

f) W przypadku pracowników wykonujących zadania wykraczające poza standardowy zakres obowiązków danego stanowiska (np. magazynier dostarczający paczki imiennie do mieszkańców, pokojowa pomagająca w opiece) należy:

- szczegółowo udokumentować rzeczywisty zakres zadań i powiązane z nimi kategorie danych,
- dostosować treść upoważnienia do faktycznego przetwarzania,
- wprowadzić dodatkowe środki organizacyjne (np. instrukcje, szkolenia) zapewniające, że dostęp do danych jest ograniczony do minimum niezbędnego do wykonywania konkretnego zadania.

g) Niedopuszczalne jest stosowanie ogólnych sformułowań typu „w zakresie statutowych zadań placówki" bez konkretyzacji kategorii danych i operacji przetwarzania. Takie upoważnienie nie spełnia wymagań art. 29 RODO i art. 20 Dekretu.

h) Wzór upoważnienia przedstawiono w części 4 niniejszych praktycznych wskazań.

2.7. Rejestr czynności przetwarzania

a) DPS powinien prowadzić rejestr zgodnie z art. 30 RODO oraz art. 21 Dekretu.

b) Dla każdej czynności należy wskazać m.in.:

- cele przetwarzania,
- kategorie osób i danych,
- odbiorców (zgodnie z decyzjami PUODO wymaga się **wskazania kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione** – art. 30 ust. 1 lit. d RODO),

- **konkretne planowane terminy usunięcia danych** (np. „10 lat od zakończenia pobytu”, „50 lat – dokumentacja medyczna zgodnie z ustawą o działalności leczniczej”, „3 lata od zakończenia rekrutacji”), zamiast ogólnej formuły „zgodnie z prawem”.

c) Rejestr powinien być spójny z klauzulami informacyjnymi i faktyczną praktyką archiwizacji.

d) Naruszenie wymogu zamieszczenia w rejestrze informacji o kategoriach odbiorców zostało stwierdzone w decyzjach PUODO jako naruszenie art. 30 ust. 1 lit. d RODO – tym samym DPS powinien pilnie uzupełnić te informacje we wszystkich czynnościach przetwarzania.

2.8. Szkolenia i świadomość personelu

a) Zgodnie z art. 24 i 32 RODO oraz art. 17 i 22 Dekretu, DPS powinien zapewnić **regularne szkolenia** wszystkich pracowników i osób współpracujących, którzy przetwarzają dane.

b) Szkolenia powinny obejmować w szczególności:

- zasady przetwarzania danych w DPS,
- ochronę szczególnych kategorii danych i tajemnic (tajemnica zawodowa, tajemnica duszpasterska, kan. 220 KPK, art. 9 ust. 2 pkt 3 i 4 Dekretu),
- zasady posługiwania się dokumentacją i systemami informatycznymi,
- procedury reagowania na naruszenia,
- wyniki przeglądów środków bezpieczeństwa i wnioski z naruszeń.

c) Udział w szkoleniach należy dokumentować (listy obecności, testy, zaświadczenia).

d) Szkolenia powinny być prowadzone:

- wstępnie – przed dopuszczeniem osoby do przetwarzania danych,
- okresowo – co najmniej raz w roku lub częściej, gdy występują istotne zmiany przepisów, procedur wewnętrznych,
- po incydentach związanych z nieprawidłowym przetwarzaniem danych osobowych.

e) **Konsekwencje braku regularnych szkoleń**:

- Brak regularnych szkoleń lub szkolenie jedynie części pracowników przetwarzających dane stanowi naruszenie art. 24 ust. 1 i 2 i art. 32 ust. 4 RODO oraz 17 ust. 1-2 i 22 ust. 3 Dekretu (w kontekście zapewnienia, aby osoby przetwarzające dane działające z upoważnienia administratora rozumiały swoje obowiązki).

- W praktyce orzeczniczej PUODO stwierdzono, że szkolenie przeprowadzone wiele lat wcześniej i obejmujące tylko niewielki odsetek zatrudnionych pracowników nie spełnia wymogu „regularnych szkoleń” i stanowi dowód na niewdrożenie odpowiednich środków organizacyjnych.

f) **Dokumentowanie szkoleń**:

- DPS powinien prowadzić rejestr szkoleń zawierający: datę szkolenia, listę uczestników (z podpisami), zakres tematyczny (program szkolenia), osobę prowadzącą szkolenie, materiały szkoleniowe (prezentacje, instrukcje).
- Dokumentacja ta powinna być dostępna do wglądu organu nadzorczego w ramach kontroli, jako dowód realizacji obowiązku wynikającego z art. 24 i 32 RODO.

g) **Praktyczne formy szkoleń**:

- Szkolenie wstępne (przed dopuszczeniem do przetwarzania): obejmujące podstawy RODO i Dekretu, politykę DPS, upoważnienia, procedury bezpieczeństwa.
- Szkolenie okresowe (coroczne): przypomnienie zasad, omówienie zmian w przepisach, omówienie przypadków naruszeń i dobrych praktyk.
- Szkolenia doraźne: gdy występują istotne zmiany przepisów, przy istotnych zmianach organizacyjnych, po wystąpieniu naruszenia, przy wdrażaniu nowych systemów IT.

2.9. Naruszenia ochrony danych

a) Każdy DPS powinien mieć określony sposób postępowania na wypadek wystąpienia naruszenia, zanim takie naruszenie nastąpi (regulacje zawarte w polityce ochrony danych lub osobnej instrukcji itp.). Powinno być wiadome, jakie czynności należy podjąć w przypadku wystąpienia naruszenia celem naprawienia sytuacji. Kolejnym etapem jest wyciągnięcie wniosków z zaistniałego naruszenia, co może skutkować zmianą procedur, dodatkowymi szkoleniami, a także konsekwencjami dla osoby, która dopuściła się naruszenia lub innymi.

b) W przypadku naruszenia ochrony danych DPS musi stosować równocześnie:

- procedury z art. 33–34 RODO (zgłoszenie naruszenia PUODO, zawiadomienie osób, jeżeli może powodować wysokie ryzyko naruszenia ich praw lub wolności),

- procedury z art. 27–28 Dekretu (zgłoszenie naruszenia Kościelnemu Inspektorowi Ochrony Danych, zawiadomienie osób, jeżeli może powodować wysokie ryzyko naruszenia ich praw lub wolności).

c) Należy prowadzić **rejestr naruszeń** zawierający dane wymagane przez art. 33 ust. 5 RODO oraz art. 27 ust. 5 Dekretu (okoliczności naruszenia, jego skutki lub możliwe skutki, uzasadnienie oceny ryzyka oraz podjęte działania zaradcze i zapobiegawcze, szczegóły dotyczące zgłoszenia naruszenia do PUODO lub KIOD, albo uzasadnienie decyzji o niezgłaszaniu, szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu lub uzasadnienie decyzji o niezgłoszeniu, ewentualnie możliwe także: kategorie i przybliżona liczba osób, kategorie i przybliżona liczba wpisów, prawdopodobne konsekwencje, środki zaradcze – dokumentowanie naruszeń zostało opisane w poradniku PUODO pt. „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" w rozdziale 8 „Dokumentowanie naruszeń ochrony danych osobowych" str. 73–76; https://uodo.gov.pl/pl/138/3561).

d) Zgłoszenie naruszenia do PUODO i KIOD powinno nastąpić bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

e) Zawiadomienie osób, których dane dotyczą, jest obowiązkowe, gdy naruszenie może powodować wysokie ryzyko naruszenia ich praw lub wolności (art. 34 RODO; art. 28 Dekretu) np. w sytuacji, gdy po zakończeniu umowy o pracę DPS wyśle świadectwo pracy do niewłaściwego adresata lub gdy dokumentacja mieszkańców zawierająca dane w postaci PESEL i danych szczególnych ulegnie ujawnieniu.

2.10. Przechowywanie danych i ograniczenie czasu przetwarzania

2.10.1. Dokumentacja pracownicza

a) DPS musi:

- przechowywać dokumentację pracowniczą **nie dłużej niż przez okres wynikający z właściwych przepisów prawa pracy, ubezpieczeń społecznych, przepisów podatkowych i archiwizacji**,
- zapewnić zgodność pomiędzy terminami wskazanymi w rejestrze czynności, politykach i faktyczną praktyką przechowywania.

b) Przechowywanie dokumentacji dłużej niż jest to wymagane narusza zasadę ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO; art. 6 ust. 1 pkt 5 Dekretu) i zostało wprost wskazane jako nieprawidłowość w decyzjach PUODO.

c) DPS powinien wprowadzić procedurę regularnego przeglądu dokumentacji (np. corocznie) w celu identyfikacji dokumentów, dla których upłynął okres przechowywania, oraz ich usunięcia lub przekazania do archiwum zakładowego/państwowego zgodnie z przepisami archiwalnymi.

d) DPS powinien wdrożyć procedurę regularnego przeglądu dokumentacji pracowniczej:

- wyznaczenie osoby odpowiedzialnej za przegląd (np. kierownik ds. kadr),
- ustalenie harmonogramu przeglądów (co najmniej raz w roku, najlepiej w stałym terminie – w określonym miesiącu każdego roku),
- przygotowanie listy dokumentacji podlegającej zniszczeniu (z wyszczególnieniem: nazwisko pracownika, data zakończenia zatrudnienia, data upływu okresu przechowywania, podstawa prawna okresu),
- protokolarne zniszczenie dokumentacji (protokół zniszczenia podpisany przez co najmniej dwie osoby, z wymienieniem kategorii zniszczonych dokumentów),
- prowadzenie rejestru zniszczonej dokumentacji, np. data zniszczenia danych, określenie niszczonych danych, np. „Akta osobowe – rok …".

e) Przykładowy harmonogram niszczenia:

- Akta osobowe pracowników: przegląd w roku N dotyczy osób, które zakończyły zatrudnienie do 31.12. roku N-11 (dla okresu 10 lat),
- Listy płac i dokumentacja wynagrodzeń: przegląd w roku N dotyczy dokumentacji za rok N-6 (dla okresu 5 lat przewidzianego przepisami podatkowymi).

2.10.2. Dane mieszkańców i innych osób

a) Dla dokumentacji mieszkańców oraz innych kategorii danych DPS powinien:

- ustalić konkretne terminy przechowywania lub jasne kryteria (np. „10 lat od zakończenia pobytu", „okres wynikający z ustawy o narodowym zasobie archiwalnym i archiwach"),
- wpisać je do rejestru czynności i klauzul informacyjnych,
- wdrożyć praktyczne procedury usuwania lub anonimizacji danych po upływie tych okresów.

b) Rejestrowanie jedynie formuły „zgodnie z przepisami prawa” utrudnia rozliczalność i może zostać uznane za naruszenie art. 30 ust. 1 lit. f RODO i art. 21 Dekretu.

c) Dla dokumentacji medycznej wytwarzanej przez DPS (patrz: pkt 1.6) należy stosować zróżnicowane okresy przechowywania:

- dokumentacja medyczna ogólna: 20 lat od zakończenia roku kalendarzowego, w którym dokonano ostatniego wpisu (art. 29 ust. 1 ustawy o działalności leczniczej),
- dokumentacja dzieci do ukończenia 18. roku życia lub do ukończenia 22. roku życia w przypadku kontynuowania nauki: odpowiednio dłużej,

UWAGA: Co do zasady DPS prowadzi dokumentację pielęgnacyjną i opiekuńczą. DPS może przechowywać dokumentację medyczną gromadzoną przez pacjenta (np. wyniki badań, wypisy ze szpitala, zalecenia medyczne). W tych przypadkach dokumentacja medyczna znajduje się w aktach mieszkańca i wówczas okres jej przechowywania pokrywa się z okresem przechowania dokumentacji mieszkańca.

UWAGA: DPS powinien prowadzić osobny rejestr dokumentacji medycznej wytwarzanej przez DPS zawierający informację o dacie założenia dokumentacji, dacie ostatniego wpisu oraz planowanej dacie zniszczenia, aby umożliwić przestrzeganie terminów wynikających z przepisów.

3. PYTANIA I ODPOWIEDZI

3.1. Czy administratorem danych jest DPS czy zgromadzenie zakonne?

Co do zasady administratorem danych przetwarzanych w ramach działalności DPS (np. mieszkańców i osób zatrudnionych przez DPS, w rozumieniu art. 4 pkt 7 RODO i art. 5 pkt 4 Dekretu, nie jest **kościelna publiczna osoba prawna** (np. zgromadzenie zakonne, diecezja), która prowadzi DPS, lecz **Dom Pomocy Społecznej** jako jednostka organizacyjna tej osoby prawnej.
DPS bowiem decyduje o celach oraz sposobach przetwarzania danych. Takie rozwiązanie zostało też przyjęte w praktyce KIOD i PUODO. Dyrektor DPS działa jako przedstawiciel administratora, czyli DPS. Dla przejrzystości zaleca się, aby w klauzulach informacyjnych i dokumentach wewnętrznych wskazywać jednoznacznie: „Administratorem Pani/Pana danych jest Dom Pomocy Społecznej [dalsza nazwa] w [miejscowość]".

3.2. Na jakiej podstawie prawnej DPS może przetwarzać dane medyczne mieszkańców?

Dane medyczne mieszkańców DPS może przetwarzać na podstawie:

a) RODO: art. 9 ust. 2 lit. b, g, h (opieka zdrowotna, zabezpieczenie społeczne, interes publiczny).

UWAGA: Przykładowe podstawy prawne przetwarzania zob. klauzula informacyjna dla mieszkańców DPS – pkt 4.1.

b) Dekret: art. 7 ust. 1 pkt 3 i 5 (obowiązek prawny i zadanie w interesie publicznym), art. 7 ust. 2 (dane wrażliwe przetwarzane w ramach uprawnionej działalności Kościoła).

Nie jest konieczne pozyskiwanie odrębnej zgody, jeżeli przetwarzanie jest niezbędne do realizacji ustawowych zadań DPS i udzielania opieki. Zgoda może być przydatna w przypadkach wykraczających poza podstawowe zadania, np. udział w programach badawczych, publikacja przypadków medycznych w celach edukacyjnych.

3.3. Czy DPS może przekazywać informacje o mieszkańcu członkom jego rodziny?

Co do zasady nie jest dozwolone przekazywanie danych o mieszkańcu członkowi jego rodziny lub opiekunowi faktycznemu. Przekazywanie tych informacji jest dopuszczalne, gdy:

a) wynika z przepisów prawa (np. opiekun prawny, kurator),
b) jest niezbędne do realizacji celu związanego z opieką (interes żywotny mieszkańca – art. 6 ust. 1 lit. d RODO; art. 7 ust. 1 pkt 4 Dekretu),
c) w innych przypadkach – na podstawie zgody mieszkańca, jeżeli jest zdolny do jej wyrażenia (art. 6 ust. 1 lit. a RODO; art. 7 ust. 1 pkt 1 Dekretu).

Zakres przekazywanych informacji powinien być ograniczony do niezbędnego minimum (zasada minimalizacji – art. 5 ust. 1 lit. c RODO; art. 6 ust. 1 pkt 3 Dekretu).

W praktyce DPS powinien mieć regulamin kontaktu z rodzinami określający, w jakich okolicznościach i w jakim zakresie informacje są udostępniane.

3.4. Czy DPS powinien wyznaczyć inspektora ochrony danych?

Zgodnie z art. 37 ust. 1 lit. b RODO oraz art. 30 ust. 1 Dekretu, podmiot przetwarzający dane na dużą skalę, w szczególności dane szczególnych kategorii, **powinien wyznaczyć inspektora ochrony danych**.

Możliwe jest także rozwiązanie, iż zostanie wyznaczony jeden inspektor ochrony danych dla całej kościelnej osoby prawnej (np. prowincji, zgromadzenia), któremu powierzy się obsługę działalności związanej z charyzmatem zakonnym – prowadzeniem domów pomocy społecznej. Wówczas każda z jednostek organizacyjnych kościelnej osoby prawnej może się konsultować we wszystkich sprawach z zakresu ochrony danych. „Skorzystanie z takiego rozwiązania wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora" (zob. https://uodo.gov.pl/pl/495/2406). Zapewniona musi być tzw. efektywna dostępność inspektora dla osób z danej organizacji.

3.5. Jak długo DPS może przechowywać dokumentację pracowniczą?

Dokumentacja pracownicza musi być przechowywana przez okres wynikający z przepisów prawa pracy i przepisów archiwalnych. Przechowywanie jej dłużej, niż jest to niezbędne, narusza zasadę ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO). Konkretny okres (np. 10 lat od zakończenia zatrudnienia dla większości dokumentów, 50 lat dla dokumentacji emerytalnej lub dla akt pracownika zatrudnionego przed 1 stycznia 1999 roku) powinien zostać wskazany w rejestrze czynności i w polityce ochrony danych oraz przestrzegany w praktyce.

3.6. Czy brak procedur przeglądu środków bezpieczeństwa jest naruszeniem RODO?

Tak. Brak procedur testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych został uznany przez PUODO w decyzjach organów nadzorczych za naruszenie art. 24 ust. 2 oraz art. 32 ust. 1 lit. d RODO. DPS powinien mieć pisemnie określone, jak często i w jaki sposób dokonuje się takich przeglądów, kto jest za nie odpowiedzialny oraz w jaki sposób dokumentuje się ich wyniki i wdraża działania naprawcze.

3.7. Czy DPS musi wskazywać konkretnych odbiorców danych w klauzulach informacyjnych?

Tak – co do zasady. Zgodnie z decyzjami PUODO wskazywanie ogólnikowej informacji typu „organy administracji publicznej" bez konkretyzacji stanowi naruszenie art. 5 ust. 1 lit. a (zasada przejrzystości), art. 12 ust. 1 oraz art. 13 ust. 1 lit. e i art. 14 ust. 1 lit. e RODO. DPS powinien podać **pełną nazwę i dane kontaktowe podmiotu** (np. „Starostwo [nazwa], ul. [adres]; NFZ Oddział w [nazwa], ul. [adres]"). Natomiast gdy lista jest zmienna – **szczegółowo określić kategorie odbiorców** (rodzaj działalności, sektor, lokalizacja). Zaleca się stosowanie modelu mieszanego: podanie z nazwy kluczowych odbiorców oraz szczegółowych kategorii dla pozostałych.

3.8. Czy DPS może stosować monitoring wizyjny w placówce?

Tak, ale z zastrzeżeniami. Monitoring wizyjny może być stosowany na podstawie:

a) art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes administratora – zgodnie z analizą konkretnego przypadku ochrona bezpieczeństwa osób lub mienia) – po uprzednim przeprowadzeniu testu proporcjonalności, albo
b) art. 6 ust. 1 lit. c RODO w zw. z przepisami sektorowymi (np. art. 18e ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego).

DPS powinien:

a) przeprowadzić analizę ryzyka i wyważenie interesów,
b) umieścić odpowiednie oznakowanie informujące o monitoringu (art. 13 RODO),
c) ograniczyć monitoring do obszarów niezbędnych (korytarze, wejścia, zewnętrzne tereny
d) nie wolno monitorować obszarów takich jak pokoje mieszkańców, łazienki i innych, których monitorowanie narusza godność osób nagrywanych,

e) określić i przestrzegać okresy przechowywania nagrań (do 3 miesięcy),

f) zapewnić odpowiednie zabezpieczenie nagrań,

g) uwzględnić monitoring w rejestrze czynności przetwarzania,

h) realizować obowiązek informacyjny – przekazanie przez administratora osobie, której dane dotyczą, określonych informacji (w tym m.in. na jakiej podstawie prawnej będą przetwarzane jej dane osobowe w związku ze stosowaniem monitoringu). Należy mieć również na uwadze, że monitoring może dotyczyć też pracowników DPS. Wówczas należy spełnić określone wymogi z prawa pracy (np. uzupełnienie regulaminu pracy, przedłożenie informacji pracownikowi, wprowadzenie monitoringu min. z 14 dniowym wyprzedzeniem) – art. 22(2) Kodeksu pracy.

W razie wątpliwości zaleca się konsultację z IOD.

Zaleca się również zapoznanie się z „Praktycznymi wskazaniami z dnia 13 maja 2019 r. z zakresu ochrony danych osobowych w związku z wykorzystywaniem monitoringu wizyjnego wydanymi przez KIOD przy współpracy z UODO".

3.9. Czy mieszkaniec może zażądać usunięcia swoich danych z dokumentacji prowadzonej przez DPS?

Co do zasady – nie, jeżeli przetwarzanie nie jest na podstawie zgody i jeżeli przetwarzanie jest niezbędne do wypełnienia obowiązków prawnych DPS (art. 17 ust. 3 lit. b RODO i art. 14 ust. 3 pkt 2 Dekretu) lub wykonywania zadania w interesie publicznym (art. 17 ust. 3 lit. d RODO i art. 14 ust. 3 pkt 3 Dekretu) – co ma miejsce, gdy DPS świadczy usługi w ramach zadań zleconych przez organ jednostki samorządu terytorialnego. DPS prowadzi dokumentację mieszkańców na podstawie przepisów ustawowych (np. ustawy o pomocy społecznej) i nie może jej usunąć na żądanie osoby, której dane dotyczą.

Wyjątek: jeżeli dane są przetwarzane na podstawie zgody (np. dodatkowe cele, publikacja wizerunku), osoba może cofnąć zgodę i żądać usunięcia danych w tym zakresie (art. 17 ust. 1 lit. b RODO; art. 14 ust. 1 pkt 2 Dekretu).

4. WZORY DOKUMENTÓW (DO DOSTOSOWANIA)

Poniższe wzory mają charakter pomocniczy. DPS powinien każdorazowo dostosować je do swojej struktury organizacyjnej, uwarunkowań prawnych i faktycznych.

4.1. Wzór klauzuli informacyjnej dla mieszkańca DPS

UWAGA: Z uwagi na to, że klauzula informacyjna skierowana jest do osób, których sprawność intelektualna może być ograniczona, należy zweryfikować, czy klauzula jest napisana językiem wystarczająco jasnym oraz czy inne przydatne informacje są podane w sposób czytelny, np. dane kontaktowe do organów nadzorczych – mimo, że nie ma obowiązku wskazania w treści klauzuli informacyjnej danych adresowych lub teleadresowych organu nadzorczego.

Klauzula informacyjna dotycząca przetwarzania danych osobowych mieszkańców Domu Pomocy Społecznej

1. Administrator danych

Administratorem Pani/Pana danych osobowych jest Dom Pomocy Społecznej [pełna nazwa] z siedzibą w [adres pocztowy], tel. [numer], e-mail: [adres].

2. Inspektor ochrony danych

Wyznaczony został Inspektor Ochrony Danych, z którym można się kontaktować pod adresem: [adres pocztowy lub e-mail], tel. [numer].

3. Cele i podstawy prawne przetwarzania

Pani/Pana dane osobowe i jeżeli ma to zastosowanie, także szczególne kategorie danych osobowych (dane wrażliwe) będą przetwarzane w następujących celach:

a) przyjęcie do DPS i prowadzenie dokumentacji pobytu oraz udzielanej pomocy – na podstawie art. 6 ust. 1 lit. b i c (albo) e i c RODO oraz art. 9 ust. 2 lit. b i h RODO w związku z:

UWAGA: Podstawa przetwarzania z art. 6 ust. 1 lit. e zależy od tego, czy DPS ma podpisaną umowę z jednostką samorządu terytorialnego.

– art. 100 ust. 2 ustawy z dnia 12 marca 2004 r. o pomocy społecznej;

– rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 23 sierpnia 2012 r. w sprawie domów pomocy społecznej w zakresie koniecznym do realizacji usług przez DPS: § 2 ust. 2–4 w zakresie danych koniecznych do ustalenia indywidulanych potrzeb mieszkańca DPS; § 3 ust. 1–2 w zakresie danych koniecznych do ustalenia indywidualnego planu wsparcia mieszkańca domu; § 3 ust. 2a oraz § 5 ust. 5 w zakresie danych w przypadku domu dla osób uzależnionych od alkoholu; § 5 ust. 2 w przypadku domu dla dzieci i młodzieży niepełnosprawnych intelektualnie;

– art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (w zakresie dokumentacji dotyczącej przymusu bezpośredniego lub zakazu opuszczania DPS) oraz w formie i zakresie uregulowanym w rozporządzeniu Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania;

– art. 18 ust. 1 i 2 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego – w zakresie dokumentowania przymusu bezpośredniego w zw. z rozporządzeniem Ministra Zdrowia z dnia 21 grudnia 2018 r. w sprawie stosowania przymusu bezpośredniego wobec osoby z zaburzeniami psychicznymi;

– art. 139 ust. 1 pkt 10 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (pobieranie odpłatności z świadczeń emerytalno-rentowych);

– rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 8 kwietnia 2021 r. w sprawie rodzinnego wywiadu środowiskowego w zakresie wskazanym w załącznikach do tego rozporządzenia, a także na podstawie art. 7 ust. 1 pkt 3 i 5 Dekretu (wypełnienie obowiązku prawnego; wykonywanie zadania w interesie publicznym):

a) zapewnienia opieki zdrowotnej, rehabilitacyjnej i pielęgnacyjnej – na podstawie art. 9 ust. 2 lit. b i h RODO (przetwarzanie danych szczególnych kategorii w zakresie ochrony zdrowia, zabezpieczenia społecznego) w związku z ustawą z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta – np. art. 25 tej ustawy oraz art. 7 ust. 1 pkt 3 i 5 w związku z art. 7 ust. 2 Dekretu (dane przetwarzane w ramach działalności Kościoła);

b) załatwienia spraw meldunkowych na podstawie art. 6 ust. 1 lit. c RODO oraz w związku z art. 24, 28 ust. 2 i 35 ustawy z dnia 24 września 2010 r. o ewidencji ludności;

c) rozliczenia finansowego, sprawozdawczości i archiwizacji – na podstawie art. 6 ust. 1 lit. c RODO w związku z przepisami o rachunkowości, podatkowymi oraz o narodowym zasobie archiwalnym i archiwach a także art. 7 ust. 1 pkt 3 Dekretu (wypełnienie obowiązku prawnego);

d) ustalenia, dochodzenia lub obrony roszczeń – na podstawie art. 6 ust. 1 lit. f RODO oraz art. 7 ust. 1 pkt 6 Dekretu (prawnie uzasadniony interes Administratora);

e) na podstawie zgody – jeżeli taka została udzielona (art. 7 ust. 1 pkt 1 Dekretu, art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO) w celu wskazanym w trakcie zbierania danych na podstawie tej zgody, np. przetwarzanie wizerunku, wyznania w celu ułatwienia kontaktu z duchownym odpowiedniego wyznania.

4. Odbiorcy danych

Pani/Pana dane osobowe mogą być przekazywane następującym odbiorcom lub kategoriom odbiorców:

a) organom administracji publicznej sprawującym nadzór: Starostwo Powiatowe w [nazwa], ul. [adres]; Wojewoda [nazwa]; Gmina [nazwa]; Urząd Skarbowy w [nazwa]; w przypadku DPS dla osób z zaburzeniami psychicznymi – sędzia w celu kontroli legalności przyjęcia i przebywania DPS osób z zaburzeniami psychicznymi

b) Narodowemu Funduszowi Zdrowia – Oddział Wojewódzki w [nazwa], ul. [adres];

c) podmiotom leczniczym współpracującym z DPS: [nazwa szpitala], [nazwa przychodni], lekarze specjaliści udzielający świadczeń mieszkańcom;

d) podmiotom przetwarzającym dane na podstawie umowy powierzenia (art. 28 RODO; art. 19 Dekretu): [nazwa firmy IT świadczącej usługi informatyczne], [nazwa firmy prowadzącej obsługę kadrowo-płacową], [nazwa firmy archiwizującej dokumenty].

5. Okres przechowywania danych

Pani/Pana dane będą przechowywane:

a) dokumentacja pobytu i opieki – przez okres 10 lat od zakończenia pobytu w DPS lub dłużej, jeżeli wynika to z przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (zob. art. 1 tej ustawy);

b) dokumentacja medyczna – przez okres 20 lat od zakończenia roku kalendarzowego, w którym dokonano ostatniego wpisu – w sytuacji, gdy dane dotyczą przymusu bezpośredniego lub ograniczenia możliwości opuszczenia DPS – (art. 29 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta);

c) dokumentacja finansowa i księgowa – przez okres wynikający z przepisów o rachunkowości i przepisów podatkowych (co najmniej 5 lat).

Dane nie będą przechowywane dłużej, niż jest to konieczne do realizacji wskazanych celów (art. 5 ust. 1 lit. e RODO i art. 30 ust. 1 lit f RODO; art. 6 ust. 1 pkt 5 oraz art. 21 ust. 1 pkt 6 Dekretu).

6. Prawa osoby, której dane dotyczą

Przysługują Pani/Panu następujące prawa:

a) prawo dostępu do swoich danych osobowych oraz ich kopii, czyli mogą Państwo uzyskać informacje, jakie dane są przetwarzane (art. 15 ust. 1 RODO; art. 11 Dekretu),

b) prawo do sprostowania danych, jeżeli dane osobowe są nieprawidłowe lub niekompletne (art. 16 RODO; art. 12 i 13 Dekretu),

c) prawo do usunięcia danych („prawo do bycia zapomnianym") z zastrzeżeniem wyjątków przewidzianych w art. 17 ust. 3 RODO, w szczególności, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego lub wykonywania zadania realizowanego w interesie publicznym (art. 14 Dekretu),

d) prawo do ograniczenia przetwarzania w przypadkach określonych przez prawo (art. 18 RODO; art. 15 Dekretu),

e) prawo do sprzeciwu wobec przetwarzania w przypadkach, gdy podstawą przetwarzania jest prawnie uzasadniony interes administratora z przyczyn związanych z Państwa szczególną sytuacją (art. 21 RODO; art. 220 Kodeksu Prawa Kanonicznego).

W celu realizacji swoich praw może Pani/Pan skontaktować się z Administratorem lub Inspektorem Ochrony Danych pod wskazanymi wyżej danymi kontaktowymi.

7. Prawo wniesienia skargi

Przysługuje Pani/Panu także prawo wniesienia skargi do:

a) Prezesa Urzędu Ochrony Danych Osobowych – w zakresie przetwarzania danych w związku z działalnością DPS w ramach prawa powszechnie obowiązującego (art. 77 RODO);

b) Kościelnego Inspektora Ochrony Danych – w zakresie przetwarzania danych w ramach działalności Kościoła katolickiego (art. 41 Dekretu),

w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy prawa.

8. Wymóg podania danych

Podanie danych osobowych jest wymogiem ustawowym wynikającym z przepisów ustawy z dnia 12 marca 2004 r. o pomocy społecznej (np. art. 54, 59, 100 ust. 2, art. 106), rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 23 sierpnia 2012 r. w sprawie domów pomocy społecznej (np. § 8 i § 11), ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (art. 24–25). Odmowa podania danych uniemożliwi świadczenie usług przez DPS, ustalenia odpłatności lub opracowania indywidualnego planu wsparcia.

Natomiast podanie danych osobowych przetwarzanych na podstawie zgody jest dobrowolne. Przysługuje Pani/Panu prawo do cofnięcia tej zgody (kontaktując się z Administratorem, np. pisemnie na adres podany na początku klauzuli informacyjnej) w dowolnym momencie, bez wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.

9. Zautomatyzowane podejmowanie decyzji

Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym w formie profilowania, skutkującym podejmowaniem wobec Pani/Pana decyzji wywołujących skutki prawne lub w podobny sposób istotnie wpływających na Pani/Pana sytuację.

UWAGA: Jeżeli DPS przetwarza dane w sposób automatyzowany, to należy w pkt 6 klauzuli informacyjnej dodać informacje o prawie do przenoszenia danych (art. 20 RODO), jeżeli przetwarzanie odbywa się na podstawie zgody lub umowy oraz w sposób zautomatyzowany.

4.2. Wzór klauzuli informacyjnej dla pracownika

Klauzula informacyjna

dotycząca przetwarzania danych osobowych pracowników

1. Administrator danych

Administratorem Pani/Pana danych osobowych jest Dom Pomocy Społecznej [pełna nazwa] z siedzibą w [adres pocztowy], tel. [numer], e-mail: [adres].

2. Inspektor ochrony danych

Wyznaczony został Inspektor Ochrony Danych, z którym można się kontaktować pod adresem: [adres pocztowy lub e-mail], tel. [numer].

3. Cele i podstawy prawne przetwarzania

Pani/Pana dane osobowe będą przetwarzane w następujących celach:

a) w celu przygotowania i realizacji umowy o pracę – na podstawie art. 6 ust. 1 lit. b RODO (działania podejmowane na żądanie osoby, której dane dotyczą, przed zawarciem umowy) oraz art. 7 ust. 1 pkt 2 Dekretu;

b) w celu zawarcia i wykonania umowy o pracę lub innej umowy (art. 6 ust. 1 lit. b RODO; art. 7 ust. 1 pkt 2 Dekretu);

c) w celu wypełnienia obowiązków spoczywających na administratorze a szczególnie wynikających z przepisów prawa pracy, ubezpieczeń społecznych, przepisów podatkowych oraz przepisów BHP (art. 6 ust. 1 lit. c RODO; art. 7 ust. 1 pkt 3 Dekretu) w szczególności w zw. z:

- art. 22^1 §1– §3 ustawy z 26 czerwca 1974 r. Kodeks pracy – dane pracownika,
- archiwizacją dokumentacji pracowniczej: art. 94 ust. 9b ustawy z dnia 26 czerwca 1974 r. Kodeks pracy w zw. z rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej,
- prawem ubezpieczeń społecznych, zabezpieczenia społecznego i ochrony socjalnej, szczególnie obowiązków zawartych art. 6 i art. 36 w zw. z art. 1 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych – zgłoszenia do ZUS,
- archiwizacją list płac, kart wynagrodzeń albo innych dowodów, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty ubezpieczonego: art. 125a ust. 4, 4a i 4b ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych – obowiązki płatników składek,
- archiwizacją dokumentacji zgłoszeniowej do ZUS: art. 36 ust. 8 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych – archiwizacja zgłoszenia do ubezpieczeń społecznych,
- archiwizacją dokumentacji rozliczeniowej z ZUS: art. 47 ust. 3c z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych – archiwizacja kopii deklaracji rozliczeniowych i imiennych raportów miesięcznych oraz dokumentów korygujących te dokumenty,

- archiwizacją karty wynagrodzeń pracownika lub ich odpowiedników: art. 74 ust. 2 pkt 2 ustawy z dnia 29 września 1994 r. o rachunkowości – okresy przechowywania danych,

a) w celu ustalenia, dochodzenia lub obrony roszczeń (art. 6 ust. 1 lit. f RODO; art. 7 ust. 1 pkt 6 Dekretu) – prawnie uzasadniony interes Administratora, jeżeli ze specyfiki relacji administrator–osoba fizyczna można racjonalnie przyjąć, że przetwarzanie danych jest niezbędne do zrealizowania przez administratora celu wynikającego z tej relacji, chyba że interesy lub podstawowe prawa i wolności osoby, której przetwarzane dane dotyczą, będą nadrzędne wobec interesu administratora.

Dane szczególnych kategorii (np. dane o zdrowiu w zakresie badań profilaktycznych) przetwarzane są na podstawie art. 9 ust. 2 lit. b RODO (wypełnianie obowiązków pracodawcy) oraz art. 7 ust. 2 Dekretu w zw. z art. 229 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

Administrator może przetwarzać Pani/Pana dane osobowe i, jeżeli ma to zastosowanie, szczególne kategorie danych osobowych (dane wrażliwe) na podstawie zgody (art. 7 ust. 1 pkt 1 Dekretu, art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO, art. 7 ust. 2 Dekretu), gdy to zostało wyraźnie zaznaczone na odpowiednim formularzu przeznaczonym do pozyskiwania danych osobowych i dotyczyć może danych w szczególności takich jak: prywatny numer telefonu lub prywatny e-mail i innych danych, o których mowa w art. 22(1a) Kodeksu pracy.

Podane tych danych osobowych własnych jest wówczas dobrowolne.

Przysługuje Pani/Panu prawo do cofnięcia tej zgody (kontaktując się z Administratorem, np. pisemnie na adres podany na początku klauzuli informacyjnej) w dowolnym momencie, bez wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.

Konsekwencją niepodania danych lub wycofania zgody na ich przetwarzanie może być uniemożliwienie podjęcia działań przez Administratora.

4. Odbiorcy danych

Pani/Pana dane osobowe mogą być przekazywane następującym odbiorcom lub kategoriom odbiorców:

a) organy administracji publicznej: Zakład Ubezpieczeń Społecznych, Urząd Skarbowy w [nazwa], Państwowa Inspekcja Pracy;

b) banki i instytucje finansowe obsługujące przelewy wynagrodzeń;

c) podmioty świadczące usługi medycyny pracy: [nazwa podmiotu wykonującego badania profilaktyczne];

d) podmioty przetwarzające dane na podstawie umowy powierzenia (art. 28 RODO; art. 19 Dekretu): [nazwa firmy prowadzącej obsługę kadrowo-płacową], [nazwa firmy świadczącej usługi IT].

5. Okres przechowywania danych

Pani/Pana dane będą przechowywane:

a) dokumentacja związana z zatrudnieniem – przez okres 10 lat od zakończenia zatrudnienia liczony od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł (zgodnie z art. 94 ust. 9b ustawy z dnia 26 czerwca 1974 r. Kodeks pracy i rozporządzeniem Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej;

b) w przypadku list płac, kart wynagrodzeń albo innych dowodów, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty ubezpieczonego – przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy: art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, chyba, że zachodzi okoliczność zgłoszenia Pani /Pana jako ubezpieczonego po dniu 31 grudnia 2018 r. wówczas będzie to 10 lat: art. 125a ust. 4, 4a, 4b ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych), chyba że odrębne przepisy przewidują inny okres przechowywania;

c) w przypadku dokumentacji rozliczeniowej z ZUS – przez okres 5 lat, licząc od dnia ich przekazania do ZUS: na podstawie art. 47 ust. 3c ustawy 13 października 1998 r. o systemie ubezpieczeń społecznych;

d) gdy chodzi o dane przetwarzane na podstawie uzasadnionego interesu administratora to będą one przetwarzane w celu ustalenia, dochodzenia lub obrony roszczeń wynikających ze stosunku pracy – 3 lata liczone od dnia, w którym roszczenie wobec pracodawcy z tytułu pracy stało się wymagalne (art. 291 ustawy Kodeks pracy) lub jeżeli dane będą przetwarzane w celu ustalenia, dochodzenia lub obrony roszczeń wynikających ze szkody wyrządzonej czynem niedozwolonym – 10 lat, licząc od dnia, w którym nastąpiło zdarzenie wywołujące szkodę: art. 442(1) ustawy Kodeks cywilny, przy czym ustalenie niezbędności przetwarzania danych osobowych opiera się

na przesłankach konkretnych, uwzględniających możliwie najszersze spektrum uwarunkowań jego realizacji. Zastosowanie tej przesłanki wymaga od administratora wykazania, że jest to konieczne z uwagi na charakter celu, okoliczności faktyczne i prawne jego realizacji oraz relacje podmiotowe pomiędzy administratorem a osobą, której te dane dotyczą.

UWAGA: Zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO), a także zasadą ograniczonego celu przetwarzania (art. 5 ust. 1 lit. b RODO) i zasady minimalizacji przetwarzania danych (art. 5 ust. 1 lit. c RODO), administrator musi umieć wykazać, że zarówno zakres, jak i sposób przetwarzania danych osobowych jest adekwatny do obranego przez niego celu i warunków jego realizacji.

6. Prawa osoby, której dane dotyczą

Przysługują Pani/Panu następujące prawa:

a) prawo dostępu do swoich danych osobowych oraz ich kopii, czyli mogą Państwo uzyskać informacje, jakie dane są przetwarzane (art. 15 ust. 1 RODO; art. 11 Dekretu),

b) prawo do sprostowania danych, jeżeli dane osobowe są nieprawidłowe lub niekompletne (art. 16 RODO; art. 12 i 13 Dekretu),

c) prawo do usunięcia danych („prawo do bycia zapomnianym") z zastrzeżeniem wyjątków przewidzianych w art. 17 ust. 3 RODO, w szczególności, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego lub wykonywania zadania realizowanego w interesie publicznym (art. 14 Dekretu),

d) prawo do ograniczenia przetwarzania w przypadkach określonych przez prawo (art. 18 RODO; art. 15 Dekretu),

e) prawo do sprzeciwu wobec przetwarzania, w przypadkach, gdy podstawą przetwarzania jest prawnie uzasadniony interes administratora z przyczyn związanych z Państwa szczególną sytuacją (art. 21 RODO; art. 220 Kodeksu Prawa Kanonicznego),

f) prawo do cofnięcia zgody – w zakresie, w jakim przetwarzanie odbywa się na podstawie zgody (cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej cofnięciem).

7. Prawo wniesienia skargi

Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (art. 77 RODO) oraz – w zakresie przetwarzania danych w ramach działalności

Kościoła – do Kościelnego Inspektora Ochrony Danych (art. 77 RODO; art. 41 Dekretu), jeżeli Pani/Pan uzna, że przetwarzanie danych osobowych narusza przepisy prawa.

8. Wymóg podania danych

Podanie danych osobowych w zakresie wynikającym z art. 22^1 Kodeksu pracy jest wymogiem ustawowym. Podanie dodatkowych danych (poza katalogiem ustawowym) jest dobrowolne i wymaga Pani/Pana zgody. Odmowa podania danych wymaganych przepisami prawa uniemożliwi zawarcie umowy o pracę.

9. Zautomatyzowane podejmowanie decyzji

Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym w formie profilowania, skutkującym podejmowaniem wobec Pani/Pana decyzji wywołujących skutki prawne lub w podobny sposób istotnie wpływających na Pani/Pana sytuację.

UWAGA: Jeżeli DPS przetwarza dane w sposób automatyzowany, to należy w pkt 6 klauzuli informacyjnej dodać informacje o prawie do przenoszenia danych (art. 20 RODO), jeżeli przetwarzanie odbywa się na podstawie zgody lub umowy oraz w sposób zautomatyzowany.

10. Inne sytuacje

Jeżeli w ramach stosunku pracy Pan/Pani będzie miał/a być dopuszczony/a do działalności obejmującej czynności związane z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, to Administrator będzie potrzebował dodatkowe Pana/Pani dane i przetwarzał je na podstawie prawa w celu realizacji swoich obowiązków ustawowych. Podstawą przetwarzania tych danych będzie więc obowiązek prawny administratora (art. 6 ust. 1 lit. c RODO oraz art. 7 ust. 1 pkt 3 Dekretu) wyrażony w szczególności w art. 21 oraz art. 23 i art. 23b ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym. W takim przypadku zostanie Pan/Pani poinformowany/a w szerszym zakresie o tym procesie przetwarzania.

4.3. Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

[Miejscowość], dnia [data]

Na podstawie art. 29 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) oraz art. 20 Dekretu ogólnego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim,

upoważniam

Panią/Pana: ……
[imię i nazwisko]

zatrudnioną/ego na stanowisku: …….
w Domu Pomocy Społecznej [nazwa],

do przetwarzania danych osobowych zgodnie z zajmowanym stanowiskiem i przydziałem czynności oraz poleceniem przełożonego, w następującym zakresie:

1. Kategorie osób, których dane dotyczą:

a) mieszkańcy DPS,

b) członkowie rodzin i opiekunowie mieszkańców,
[inne – dostosować do faktycznego zakresu]

2. Kategorie danych osobowych:

a) dane identyfikacyjne i kontaktowe mieszkańców (imię, nazwisko, PESEL, adres, telefon),

b) dane dotyczące pobytu w DPS (data przyjęcia, zakres świadczonej opieki),

c) dane dotyczące zdrowia w zakresie niezbędnym do wykonywania obowiązków pielęgnacyjnych i opiekuńczych (informacje o schorzeniach, ordynacjach lekarskich, podawaniu leków, przebiegu leczenia),
[inne – dostosować do faktycznego zakresu]

3. Operacje przetwarzania:

a) zbieranie i utrwalanie danych,

b) przeglądanie i odczytywanie danych,

c) aktualizowanie i uzupełnianie danych,

d) sporządzanie notatek, wydruków i raportów w systemie informatycznym,

e) przekazywanie danych innym upoważnionym osobom w DPS w zakresie koniecznym do realizacji zadań.

4. Ograniczenia:

a) Osoba upoważniona **nie jest uprawniona** do samodzielnego przekazywania danych osobowych poza DPS (w tym do organów, instytucji zewnętrznych, członków rodzin), chyba że wynika to wprost z jej obowiązków służbowych i zostało uregulowane w odrębnych procedurach.

b) Osoba upoważniona **nie jest uprawniona** do przetwarzania danych kadrowych pracowników DPS oraz danych finansowych DPS, chyba że stanowi to część jej obowiązków służbowych.

5. Obowiązek poufności:

Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie trwania zatrudnienia, jak i po jego zakończeniu (art. 20 ust. 2 Dekretu; art. 32 ust. 4 RODO).

Osoba upoważniona zobowiązana jest do przetwarzania danych osobowych wyłącznie w celach służbowych, zgodnie z instrukcjami Administratora oraz obowiązującymi w DPS procedurami ochrony danych.

6. Okres obowiązywania:

Niniejsze upoważnienie obowiązuje od dnia [data] do dnia [data] / do odwołania / do zakończenia zatrudnienia.

7. Oświadczenie osoby upoważnionej:

Oświadczam, że zapoznałam/em się z treścią niniejszego upoważnienia oraz z obowiązującymi w DPS procedurami ochrony danych osobowych. Zobowiązuję się do przestrzegania zasad ochrony danych osobowych oraz zachowania ich w tajemnicy oraz informacji o ich zabezpieczeniu, również po zakończeniu umowy łączącej mnie z Administratorem lub wykonaniu polecenia. Znam i rozumiem moje obowiązki wynikające z prawa powszechnie obowiązującego i prawa kanonicznego oraz regulacji wewnętrznych obowiązujących u Administratora, oraz zostałem poinformowana/y, rozumiem i znam konsekwencje nieprzestrzegania prawa w zakresie danych osobowych lub niedopełnienia obowiązków wynikających z niniejszego oświadczenia na podstawie przepisów prawa powszechnie obowiązującego, a w szczególności, gdy ma to zastosowanie: ustawy o ochronie danych

osobowych z 2018 r., Kodeksu cywilnego i Kodeksu karnego oraz prawa kanonicznego, a także odpowiedzialności w obszarze dyscyplinarnym.

……

[podpis osoby upoważnionej]

……

[podpis osoby udzielającej upoważnienia – Dyrektor DPS lub osoba upoważniona]

4.4. Podstawowe elementy umowy powierzenia przetwarzania danych

Umowa zawierana z podmiotem przetwarzającym, zgodnie z art. 28 ust. 3 RODO i art. 19 Dekretu, powinna obejmować co najmniej:

1. Oznaczenie stron: administrator: Dom Pomocy Społecznej [nazwa] - Podmiot przetwarzający: [nazwa firmy].

2. Przedmiot umowy: opis usług świadczonych przez podmiot przetwarzający (np. „obsługa systemu informatycznego zarządzania dokumentacją mieszkańców", „prowadzenie obsługi kadrowo-płacowej").

3. Czas trwania przetwarzania: okres obowiązywania umowy z oznaczeniem daty rozpoczęcia i zakończenia lub wskazaniem, że umowa jest zawarta na czas nieokreślony.

4. Charakter i cel przetwarzania: szczegółowy opis, w jakim celu podmiot przetwarzający będzie przetwarzał dane (np. „w celu zapewnienia funkcjonowania systemu informatycznego").

5. Rodzaj danych osobowych i kategorie osób, których dane dotyczą: np. „dane identyfikacyjne, kontaktowe i dane dotyczące zdrowia mieszkańców DPS; dane kadrowe pracowników DPS".

6. Obowiązek przetwarzania danych wyłącznie na udokumentowane polecenie Administratora: postanowienie, że podmiot przetwarzający przetwarza dane wyłącznie na podstawie pisemnych lub elektronicznych poleceń Administratora, chyba że obowiązek przetwarzania nakładają na niego przepisy prawa.

7. Obowiązek zapewnienia poufności przez osoby upoważnione: zobowiązanie podmiotu przetwarzającego do zapewnienia, że osoby upoważnione do przetwarzania danych zobowiążą się do zachowania tajemnicy lub będą objęte odpowiednim obowiązkiem ustawowym zachowania tajemnicy

8. Opis środków bezpieczeństwa: ogólny opis środków technicznych i organizacyjnych wdrożonych przez podmiot przetwarzający w celu zapewnienia odpowiedniego poziomu bezpieczeństwa (zgodnie z art. 32 RODO; art. 22 Dekretu).

9. Zasady korzystania z dalszych podmiotów przetwarzających (podprocesorów): wymóg uzyskania uprzedniej zgody Administratora (ogólnej lub szczegółowej) na zaangażowanie podprocesora. Zobowiązanie podmiotu przetwarzającego do nałożenia na podprocesora takich samych obowiązków ochrony danych, jakie wynikają z umowy powierzenia.

10. Pomoc Administratorowi w realizacji obowiązków: zobowiązanie podmiotu przetwarzającego do udzielania pomocy Administratorowi (oraz sposobu i terminu udzielania tej pomocy) w: a) realizacji obowiązków informacyjnych wobec osób, których dane dotyczą, b) realizacji praw osób, których dane dotyczą (dostęp, sprostowanie, usunięcie itd.), c) zgłaszaniu naruszeń ochrony danych do organu nadzorczego, d) przeprowadzaniu oceny skutków dla ochrony danych (jeśli dotyczy).

11. Obowiązek usunięcia lub zwrotu danych po zakończeniu świadczenia usług: postanowienie, że po zakończeniu świadczenia usług podmiot przetwarzający usuwa wszelkie dane osobowe lub zwraca je Administratorowi oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych.

12. Prawo Administratora do kontroli i audytu: zobowiązanie podmiotu przetwarzającego do udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków oraz do poddania się audytom i inspekcjom prowadzonym przez Administratora lub upoważnionego audytora.

13. Odpowiedzialność podmiotu przetwarzającego: postanowienie dotyczące odpowiedzialności za naruszenie obowiązków wynikających z RODO, Dekretu oraz umowy powierzenia.

14. Postanowienia końcowe: prawo właściwe, tryb rozwiązywania sporów, sposób dokonywania zmian w umowie.

KONFERENCJA
EPISKOPATU
POLSKI

KOŚCIELNY INSPEKTOR OCHRONY DANYCH