WZORZEC UMOWNY

Regulamin świadczenia usługi

Wersja 2026-09-17 · §1 Definicje

Regulamin określa zasady świadczenia przez ClinikAI usługi **„recepcja AI"** na rzecz placówek medycznych i weterynaryjnych; dotyczy wyłącznie relacji **B2B**. Jest **wzorcem umownym w rozumieniu art. 384 KC** i wiąże Klienta, który podpisał Umowę odsyłającą do jego oznaczonej wersji, udostępnionej mu przed podpisaniem. Jego rozdział **„Powierzenie przetwarzania danych osobowych" (§12–§20) stanowi umowę powierzenia w rozumieniu art. 28 RODO**. Nie stosuje się do Klienta związanego odrębną Umową Generalną ClinikAI. W razie rozbieżności pierwszeństwo mają kolejno: rozdział o powierzeniu (wyłącznie w sprawach ochrony danych), Umowa, pozostała treść Regulaminu.

§1 Definicje

- **Dostawca / ClinikAI** — **Piotr Kluch**, prowadzący działalność gospodarczą pod firmą **PK Systems Piotr Kluch**, ul. Leszczynowa 9, 95-200 Pabianice, NIP 7312013335, REGON 521021415 (CEIDG).
- **Klient** — placówka korzystająca z Usługi; **administrator** danych osób, które się z nią kontaktują.
- **Umowa** — dokument podpisany przez obie Strony: pakiet, wynagrodzenie, termin uruchomienia.
- **Usługa** — oprogramowanie SaaS, w którym **Asystent AI** obsługuje w imieniu Klienta połączenia i komunikację recepcyjną, a personel korzysta z **Panelu**.

§2 Zakres Usługi

1. **Asystent AI działa wyłącznie recepcyjnie:** odbiera połączenia, umawia, przekłada i odwołuje wizyty, udziela informacji o godzinach, usługach i organizacji pracy placówki, wysyła przypomnienia i potwierdzenia, a sprawy wymagające udziału człowieka przekazuje personelowi wraz z notatką z rozmowy.
2. **Usługa NIE obejmuje:** dokumentacji medycznej ani EDM, e-recepty, e-skierowania, dostępu do kartoteki; porad medycznych, rozpoznania, zalecania leczenia ani oceny stanu zdrowia. Sytuacje pilne Asystent rozpoznaje **według reguł Klienta**, a w sprawach nagłych kieruje do placówki albo pod numer alarmowy.
3. **Nadzór człowieka.** Decyzje merytoryczne i organizacyjne należą wyłącznie do personelu Klienta, który ma wgląd w historię rozmów i może przejąć sprawę w dowolnym momencie.
4. **Nagrywanie rozmów** jest domyślnie **wyłączone**. Włącza je udokumentowane polecenie Klienta — **wystarczy e-mail; nie wymaga to zmiany Umowy ani ponownego podpisu**. Po włączeniu rozmówca słyszy informację o nagrywaniu **na początku każdego połączenia**; nie ma konfiguracji, w której Usługa nagrywa bez zapowiedzi. Okres przechowywania nagrań ustala Klient.
5. **Przejrzystość AI.** Klient utrzymuje w rozmowie informację, że rozmówca rozmawia z asystentem AI — zgodnie z art. 50 rozporządzenia (UE) 2024/1689.

§3 Dostępność i wsparcie

1. Dostawca dokłada starań, aby Usługa była dostępna w trybie ciągłym; planowane prace serwisowe zapowiada z wyprzedzeniem. Zgłoszenia przyjmuje w dwóch trybach: **awarie Asystenta** — całodobowo, 7 dni w tygodniu, linią alarmową (telefon/SMS), z pierwszą reakcją do 1 godziny; **pozostałe zgłoszenia i zmiany konfiguracji** — e-mailem i telefonicznie w dni robocze 9:00–17:00, z pierwszą reakcją do 1 dnia roboczego.
2. **Czasy reakcji wiążą; poziom dostępności nie jest gwarantowany.** Czasy z ust. 1 są zobowiązaniem umownym Dostawcy; Dostawca nie gwarantuje natomiast liczbowego poziomu dostępności ani nie przyznaje kredytów serwisowych. Zgłoszenia: **support@clinikai.pl**; ochrona danych: **rodo@clinikai.pl**.

§4 Obowiązki Klienta

1. **Rola administratora.** Klient odpowiada za podstawę prawną przetwarzania danych osób kontaktujących się z jego placówką i za zgodność korzystania z Usługi z RODO oraz z przepisami jego zawodu. Realizuje też wobec tych osób obowiązek z art. 13 RODO, korzystając z wzoru klauzuli udostępnionego przez Dostawcę.
2. **Prawdziwość danych konfiguracyjnych.** Klient odpowiada za poprawność godzin przyjęć, listy usług, personelu, zasad umawiania i danych kontaktowych.
3. **Bezpieczeństwo dostępu.** Klient zabezpiecza konta personelu i niezwłocznie zgłasza podejrzenie nieuprawnionego dostępu.
4. **Zgodne z prawem korzystanie.** Klient nie wykorzystuje Usługi do celów innych niż obsługa recepcyjna własnej placówki.
5. **Współdziałanie przy uruchomieniu.** Klient wskazuje osobę kontaktową, przekazuje godziny przyjęć, listę usług i zasady umawiania, przekierowuje numer rejestracji i kieruje zespół na szkolenie.

§5 Wynagrodzenie i rozliczenia

1. Wysokość opłat określa **Umowa**; Regulamin nie zawiera cen. Ceny są **netto**, powiększone o VAT.
2. Abonament rozliczany jest **z góry**. Fakturowanie zaczyna się z dniem produkcyjnego uruchomienia — za okres wdrożenia abonament nie jest naliczany — a uruchomienie w trakcie miesiąca rozlicza się proporcjonalnie.
3. **Przekroczenie limitu pakietu.** Jednorazowe przekroczenie limitu minut **nie powoduje dopłat**. Przekroczenie w **dwóch kolejnych miesiącach** uprawnia Dostawcę do zaproponowania wyższego pakietu — z wyprzedzeniem co najmniej 30 dni, ze wskazaniem pakietu i ceny; zmiana wchodzi w życie po potwierdzeniu przez Klienta w formie dokumentowej, a do tego czasu obowiązuje pakiet z Umowy. SMS-y ponad limit rozliczane są **z dołu**, w stawce z Umowy.
4. **Zmiana cen** wymaga powiadomienia co najmniej 30 dni wcześniej i nie działa wstecz; Klient, który jej nie akceptuje, może wypowiedzieć umowę (§10).

§6 Zawieszenie świadczenia Usługi

1. Przy opóźnieniu w zapłacie przekraczającym **14 dni** Dostawca — po wezwaniu do zapłaty z dodatkowym terminem nie krótszym niż 7 dni — może **zawiesić świadczenie Usługi** do czasu uregulowania zaległości, zachowując prawo do wynagrodzenia za zawieszony okres. Zawieszenie nie jest wypowiedzeniem; Usługa wraca niezwłocznie po zapłacie.
2. **Spór w dobrej wierze.** Prawo zawieszenia nie przysługuje co do należności zakwestionowanych przez Klienta w dobrej wierze, w formie dokumentowej i przed terminem płatności — przez **30 dni** od zgłoszenia. Część bezsporna pozostaje wymagalna; po bezskutecznym upływie tych 30 dni ust. 1 stosuje się do całości.

§7 Odpowiedzialność

1. **Charakter asystujący AI.** Usługa wspiera pracę personelu. Systemy generatywne mogą udzielić odpowiedzi nieprawidłowej lub niepełnej, a Dostawca **nie odpowiada za decyzje podjęte na podstawie wypowiedzi lub rekomendacji AI bez weryfikacji przez personel Klienta**.
2. **Ograniczenie odpowiedzialności.** Łączna odpowiedzialność Dostawcy z tytułu Usługi — w tym odpowiedzialność wynikająca z rozdziału o powierzeniu — ograniczona jest do kwoty **wyższej z dwóch**: (a) **12-krotności miesięcznego abonamentu netto** z Umowy, liczonej bez rabatów i okresów bezpłatnych, albo (b) **opłaty wdrożeniowej netto zapłaconej** przez Klienta. Wyłącza się **utracone korzyści** oraz szkody z decyzji, o których mowa w ust. 1.
3. **Czego limit nie obejmuje.** Ograniczenia z ust. 2 nie stosuje się do szkód wyrządzonych **umyślnie** albo wskutek **rażącego niedbalstwa**, do **naruszenia poufności** (§8), do **roszczeń osób trzecich o naruszenie praw własności intelektualnej**, ani tam, gdzie jest ono niedopuszczalne z mocy prawa — w tym co do art. 82 RODO.

§8 Własność intelektualna, poufność i brak wyłączności

1. System i know-how pozostają **wyłączną własnością Dostawcy**. Klient otrzymuje **niewyłączną, nieprzenoszalną licencję** na korzystanie z Usługi na czas jej świadczenia, ograniczoną do własnej działalności; Umowa nie przenosi na niego żadnych praw własności intelektualnej.
2. Dane Klienta pozostają jego własnością; ich zwrot i usunięcie opisują §10 i §16. Żadna ze Stron nie jest związana **wyłącznością**.
3. **Poufność.** Strony zachowują w poufności informacje techniczne, handlowe i know-how drugiej Strony przez czas świadczenia Usługi i **3 lata** po jego zakończeniu; nie dotyczy to informacji publicznie dostępnych ani żądanych przez uprawnione organy.
4. **Materiały Dostawcy.** Oferta, Umowa, materiały wdrożeniowe, dokumentacja Usługi oraz sposób powiązania Usługi z systemami informatycznymi Klienta są informacjami poufnymi Dostawcy. Klient nie udostępnia ich osobom trzecim — **w tym dostawcom i serwisantom swoich systemów informatycznych** — bez zgody Dostawcy w formie co najmniej dokumentowej. Nie dotyczy to: doradców prawnych, podatkowych i audytorów związanych tajemnicą zawodową; ujawnienia wymaganego prawem; osób uczestniczących we wdrożeniu na prośbę Dostawcy; ani informatyków i serwisantów Klienta w zakresie niezbędnym do eksploatacji Usługi, o ile są związani poufnością nie słabszą niż niniejszy paragraf.

§9 Ochrona danych osobowych

1. Powierzenie reguluje **rozdział „Powierzenie przetwarzania danych osobowych" (§12–§20)**: Klient jest **administratorem**, Dostawca **podmiotem przetwarzającym** (art. 28 RODO) — wyłącznie na udokumentowane polecenie Klienta i **bez wykorzystania danych do celów własnych ani do trenowania modeli AI**.
2. **Lista podprocesorów** — imienny wykaz podmiotów przetwarzających dane powierzone, z lokalizacją, mechanizmem transferu i okresem przechowywania — jest dostępna dla zalogowanych użytkowników Klienta w Panelu oraz na życzenie pod adresem **rodo@clinikai.pl**; zmienia się w trybie §14 ust. 2 i nie wymaga zmiany Umowy ani Regulaminu.
3. Prywatność ClinikAI jako administratora własnych danych opisuje **Polityka prywatności**.

§10 Okres obowiązywania, wypowiedzenie i zwrot danych

1. Umowa zawierana jest na **czas nieoznaczony**, o ile sama nie stanowi inaczej. Każda ze Stron może ją wypowiedzieć z **1-miesięcznym** okresem wypowiedzenia na koniec miesiąca — bez zobowiązania długoterminowego i bez opłat. Szersze uprawnienia z §14 ust. 2 mają pierwszeństwo.
2. **Zwrot i usunięcie danych** po zakończeniu Usługi — wedle wyboru Klienta, w **30 dni**, na zasadach **§16**; usunięcie jest **nieodwracalne**.

§11 Postanowienia końcowe

1. **Zmiany Regulaminu.** Dostawca może zmienić Regulamin, w szczególności w związku ze zmianą zakresu Usługi lub przepisów prawa. O istotnych zmianach informuje Klienta co najmniej 30 dni wcześniej (e-mailem lub w Panelu), udostępniając nową wersję; Klient, który zmiany nie akceptuje, może wypowiedzieć umowę na zasadach §10 przed dniem jej wejścia w życie. Zmiany nie działają wstecz.
2. **Następstwo prawne.** Przekształcenie, zmiana formy prawnej lub sukcesja uniwersalna po którejkolwiek ze Stron — w tym przekształcenie działalności Dostawcy w spółkę kapitałową (art. 584^1 i n. KSH) — **nie wymaga zgody drugiej Strony, nie daje podstawy do wypowiedzenia i nie rodzi opłat**; prawa i obowiązki przechodzą na następcę z mocy prawa (art. 584^2 §1 KSH).
3. **Forma, prawo i sąd.** Zmiany Umowy wymagają **co najmniej formy dokumentowej** (art. 77^2 KC), a konfigurację Usługi zmienia się e-mailem. W sprawach nieuregulowanych stosuje się Umowę i prawo polskie; właściwy jest sąd siedziby Dostawcy.

Powierzenie przetwarzania danych osobowych

Ten rozdział **stanowi umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO**, zawartą wraz z Umową, która odsyła do oznaczonej wersji Regulaminu udostępnionej Klientowi przed podpisaniem; odrębny podpis nie jest wymagany. Klient występuje tu jako **Administrator**, Dostawca jako **Podmiot przetwarzający**. Rozdział wiąże przez cały czas obowiązywania Umowy i w sprawach ochrony danych ma pierwszeństwo przed pozostałą treścią Regulaminu i Umowy. Odpowiedzialność Stron, w tym jej limit, reguluje **§7** — ten sam limit stosuje się tutaj i nie działa tam, gdzie zakazuje tego bezwzględnie obowiązujący przepis, w tym art. 82 RODO; do następstwa prawnego stosuje się §11 ust. 2.

§12 Co, po co i jak długo przetwarzamy

1. **Zakres.** Administrator powierza przetwarzanie danych w zakresie niezbędnym do świadczenia **recepcji AI**: obsługi połączeń i wiadomości w jego imieniu (umawianie, przekładanie i odwoływanie wizyt, informacje organizacyjne, wiadomości dla personelu, rozpoznanie zgłoszenia nagłego), transkrypcji rozmów i prezentacji danych w Panelu, wysyłki SMS o wizytach oraz przechowywania, kopii zapasowych i usuwania danych.
2. **Własne oprogramowanie Administratora.** Jeżeli Administrator z niego korzysta, powierzenie obejmuje także **wymianę danych z tym systemem**: odczyt terminarza i danych rejestracyjnych przy użyciu oprogramowania Podmiotu przetwarzającego uruchomionego na komputerze Administratora, a jeżeli Administrator tak ustali — również wpisy w tym terminarzu, wyłącznie dla wizyt obsłużonych w ramach Usługi i bez usuwania jego danych. Jednorazowy import danych historycznych i uruchomienie modułu dokumentacji praktyki (wraz z prowadzoną w nim dokumentacją i rejestrami) następują wyłącznie na jego polecenie.
3. **Czego Usługa nie robi** — §2 ust. 2; rozpoznanie zgłoszenia nagłego jest klasyfikacją **rejestracyjną**, a dane kliniczne i ustawowe obowiązki sprawozdawcze zostają u Administratora. **Nagrywanie rozmów** — §2 ust. 4: domyślnie wyłączone, włączane udokumentowanym poleceniem Administratora.
4. **Kategorie danych:** imię i nazwisko; numer telefonu, a gdy Administrator je zbiera — także e-mail oraz dane adresowe i rozliczeniowe; termin i status wizyty; powód wizyty podany dobrowolnie; transkrypcje rozmów; nagrania rozmów, jeżeli Administrator je włączył; dane kont personelu w Panelu. **Kategorie osób:** pacjenci albo opiekunowie zwierząt, inne osoby kontaktujące się z placówką, personel Administratora.
5. **Charakter danych i podstawa prawna Administratora (informacyjnie)** — rozstrzyga rodzaj placówki:
   a. **placówka ochrony zdrowia człowieka:** Strony przyjmują, że **sam fakt umówienia wizyty jest daną o stanie zdrowia** — ujawnia korzystanie z określonych świadczeń — niezależnie od tego, czy pacjent poda powód wizyty, więc powierzenie od początku dotyczy **danych szczególnej kategorii (art. 9 RODO)**; podstawa: art. 6 ust. 1 lit. b i f oraz art. 9 ust. 2 lit. h RODO w związku z ustawą z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
   b. **zakład leczniczy dla zwierząt:** powierzone dane to dane opiekunów zwierząt, czyli **dane zwykłe** (art. 6 ust. 1 lit. b i f, a dla dokumentacji leczenia zwierząt i rejestrów ustawowych — lit. c RODO); sam fakt umówienia wizyty zwierzęcia **nie ujawnia danych szczególnej kategorii** dotyczących osoby fizycznej, a dane zwierzęcia objęte są ochroną z tego rozdziału w zakresie powiązania z możliwym do zidentyfikowania opiekunem. Podmiot przetwarzający nie ustala własnej podstawy prawnej; obowiązek informacyjny z art. 13 RODO spoczywa na Administratorze.
6. **Czas.** Przetwarzanie trwa przez okres obowiązywania Umowy — a jeżeli Usługa ruszyła wcześniej, od dnia uruchomienia produkcyjnego — potem stosuje się §16.
7. **Obsługa zgłoszeń.** Na udokumentowane żądanie Administratora dotyczące konkretnej rozmowy upoważniony personel może zapoznać się z jej transkrypcją i nagraniem — wyłącznie po to, by rozwiązać zgłoszenie. Dane identyfikacyjne są wcześniej pseudonimizowane, każdy dostęp trafia do dziennika audytowego, a materiały są usuwane **do 30 dni od rozwiązania zgłoszenia**. Telemetria techniczna nie zawiera treści rozmów ani danych osobowych.

§13 Obowiązki Podmiotu przetwarzającego (art. 28 ust. 3 RODO)

1. **Wyłącznie na polecenie Administratora** (lit. a) — w tym co do transferów poza EOG — chyba że przetwarzania wymaga prawo UE lub państwa członkowskiego; wtedy Podmiot przetwarzający uprzedza o tym Administratora, o ile prawo nie zakazuje. Na polecenie składają się: niniejszy rozdział, Umowa z pozostałą treścią Regulaminu, uzgodniona konfiguracja Usługi, potwierdzenie uruchomienia i dalsze polecenia w formie dokumentowej.
2. **Poufność** (lit. b). Dane przetwarzają wyłącznie osoby upoważnione, w niezbędnym zakresie i zobowiązane do poufności na piśmie; rejestr upoważnień (art. 29 RODO) Podmiot przetwarzający udostępnia na żądanie. Ponadto:
   a. **w placówkach ochrony zdrowia człowieka** poufność obowiązuje na poziomie tajemnicy lekarskiej, a ten rozdział jest umową, o której mowa w **art. 24 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta**: Podmiot przetwarzający i jego personel zachowują tajemnicę **także po śmierci pacjenta** (art. 24 ust. 7 tej ustawy), a Administrator ma prawo kontroli (§17) — przetwarzanie odbywa się zatem przez osoby **związane tajemnicą na podstawie prawa krajowego w rozumieniu art. 9 ust. 3 RODO**;
   b. **w zakładach leczniczych dla zwierząt** zobowiązanie wspiera obowiązki zawodowe lekarza weterynarii z ustawy z dnia 21 grudnia 1990 r. o zawodzie lekarza weterynarii i izbach lekarsko-weterynaryjnych.
3. **Bezpieczeństwo** (lit. c) — środki techniczne i organizacyjne opisuje §20.
4. **Podpowierzenie** (lit. d) — wyłącznie na zasadach §14.
5. **Pomoc w realizacji praw osób** (lit. e) — dostęp, sprostowanie, usunięcie, ograniczenie, przenoszenie, sprzeciw; żądania kierowane wprost do Podmiotu przetwarzającego trafiają do Administratora i nie są rozstrzygane samodzielnie.
6. **Pomoc w obowiązkach art. 32–36 RODO** (lit. f) — bezpieczeństwo, zgłaszanie naruszeń (§15), ocena skutków dla ochrony danych i uprzednia konsultacja z organem nadzorczym.
7. **Zwrot albo usunięcie danych** (lit. g) — zgodnie z §16. Usunięcie następuje metodą **kryptograficznego zniszczenia klucza**, jest **nieodwracalne**, wykonywane na potwierdzone polecenie Administratora i zapisywane w dzienniku audytowym.
8. **Wykazanie zgodności i audyty** (lit. h) — na zasadach §17.
9. **Sygnalizacja.** Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli uzna, że polecenie narusza RODO.
10. **Zakaz użytku własnego i trenowania modeli.** Powierzone dane nie służą celom własnym ani trenowaniu modeli — własnych i podprocesorów. Zakaz jest **umowny i bezwarunkowy**.
11. **Kontakt: rodo@clinikai.pl.** Podmiot przetwarzający współpracuje z inspektorem ochrony danych Administratora, jeżeli go wyznaczono.

§14 Podprocesorzy

1. Administrator udziela ogólnej pisemnej zgody (art. 28 ust. 2 RODO) na korzystanie z podprocesorów wskazanych na Liście podprocesorów. Aktualna Lista podprocesorów — obejmująca dla każdego podprocesora: podmiot, zakres usługi, kategorie danych, lokalizację przetwarzania, mechanizm transferu i okres przechowywania — jest udostępniana zalogowanym użytkownikom Administratora w Panelu, a na życzenie przekazywana w wersji datowanej pod adresem **rodo@clinikai.pl**. Zmiana Listy następuje w trybie ust. 2 i nie stanowi zmiany Umowy ani Regulaminu.
2. O zamierzonym dodaniu lub zastąpieniu podprocesora Podmiot przetwarzający zawiadamia Administratora pocztą elektroniczną na adres wskazany do spraw ochrony danych co najmniej 30 dni przed rozpoczęciem przetwarzania przez nowego podprocesora, wskazując zakres usługi, lokalizację i mechanizm transferu. Administrator może w tym terminie zgłosić sprzeciw z uzasadnionych przyczyn dotyczących ochrony danych. W razie sprzeciwu, którego Strony nie rozstrzygną w terminie 14 dni,

Administrator może wypowiedzieć Umowę w zakresie objętym zmianą bez zachowania okresu wypowiedzenia i bez opłat. Podprocesorzy wskazani na Liście dostępnej w dniu zawarcia Umowy są objęci zgodą z ust. 1 z tym dniem, bez okresu zawiadomienia.

3. Z każdym podprocesorem Podmiot przetwarzający zawiera umowę o obowiązkach nie mniej rygorystycznych niż niniejszy rozdział (art. 28 ust. 4 RODO) i **odpowiada za niego jak za siebie**; jej postanowienia o ochronie danych udostępnia na żądanie w 7 dni.

§15 Zgłaszanie naruszeń

Naruszenie ochrony powierzonych danych Podmiot przetwarzający zgłasza Administratorowi **nie później niż w ciągu 24 godzin od stwierdzenia** — tak, by Administrator zdążył z własnym zgłoszeniem do organu nadzorczego (art. 33 RODO). Zgłoszenie podaje, w miarę dostępnych informacji: charakter naruszenia, kategorie i przybliżoną liczbę osób oraz rekordów, prawdopodobne konsekwencje i zastosowane środki; informacje mogą być przekazywane etapami.

§16 Zwrot i usunięcie danych

1. Po zakończeniu Usługi Podmiot przetwarzający — wedle wyboru Administratora — **zwraca** powierzone dane i/lub je **usuwa** wraz z kopiami, chyba że przechowywania wymaga prawo. Zwrot: **30 dni**, w powszechnie używanych formatach.
2. **Uczciwe zastrzeżenie.** Usunięcie danych udostępnianych w Usłudze jest natychmiastowe, ale dane identyfikacyjne mogą pozostać jako tekst jawny w historycznym rejestrze operacji i w transkrypcjach — ich usunięcie objęte jest odrębną migracją. Kopie zapasowe sprzed usunięcia mogą zawierać dane do czasu rotacji (rząd wielkości 400 dni). Dokumenty objęte retencją ustawową podlegają wyłączeniu (art. 17 ust. 3 lit. b RODO).

§17 Audyt

Administrator może żądać informacji potrzebnych do wykazania zgodności z art. 28 RODO i przeprowadzić audyt — także przez upoważnionego audytora — po uprzednim powiadomieniu i uzgodnieniu terminu, raz w roku i na swój koszt (chyba że audyt wykaże istotną niezgodność); przy istotnym incydencie — częściej. Podmiot przetwarzający może zadośćuczynić żądaniu, udostępniając ten rozdział, aktualną Listę podprocesorów, opis środków bezpieczeństwa (§20) oraz posiadane raporty i atestacje. Audyt nie może naruszać danych innych klientów.

§18 Retencja

Podmiot przetwarzający przechowuje dane przez okresy z tabeli i nie zmienia ich jednostronnie; skrócenie okresu na polecenie Administratora nie wymaga zmiany Umowy. Dokumentacja prowadzona przez Administratora zostaje u niego i podlega własnym, ustawowym okresom. Okresy u podprocesorów wskazuje Lista podprocesorów.

KATEGORIA DANYCH	OKRES PRZECHOWYWANIA
Rekordy wizyt, dane pacjenta, transkrypcje rozmów — **placówka ochrony zdrowia człowieka**	20 lat od końca roku kalendarzowego ostatniego wpisu (przez analogię do art. 29 ust. 1 ustawy o prawach pacjenta)
Rekordy wizyt, dane opiekuna, transkrypcje rozmów, dokumentacja modułu praktyki — **zakład leczniczy dla zwierząt**	okres wskazany przez Administratora co najmniej w formie dokumentowej (zakład nie dziedziczy ustawowego okresu dokumentacji medycznej człowieka); do czasu jego wskazania — czas obowiązywania Umowy; rejestry ustawowe — okres z przepisów właściwych dla zakładu
Nagrania rozmów (gdy włączone)	okres wskazany przez Administratora

KATEGORIA DANYCH	OKRES PRZECHOWYWANIA
Treść SMS / metadane doręczenia	jak transkrypcje / 12 miesięcy
Dziennik audytowy	24 miesiące
Metadane połączeń i telemetria	12 miesięcy
Materiały ze zgłoszenia (§12 ust. 7)	30 dni od rozwiązania
Rejestr żądań usunięcia / dokumenty fiskalne	5 lat
Kopie zapasowe	ok. 400 dni (§16 ust. 2)

§19 Lokalizacja danych i transfery poza EOG

1. Podmiot przetwarzający przetwarza powierzone dane na terenie Europejskiego Obszaru Gospodarczego wszędzie tam, gdzie dostawca danej usługi to umożliwia. W pozostałym zakresie dane przetwarzają podprocesorzy wskazani na Liście podprocesorów, z siedzibą lub infrastrukturą poza EOG, wyłącznie na podstawie zabezpieczeń przewidzianych w rozdziale V RODO — w szczególności standardowych klauzul umownych (art. 46 ust. 2 lit. c RODO) wraz z oceną skutków transferu i środkami uzupełniającymi opisanymi na Liście podprocesorów.
2. **Uczciwe zastrzeżenie.** Imię, nazwisko i numer telefonu wypowiedziane przez rozmówcę oraz treści podane przez niego dobrowolnie są częścią strumienia audio i transkrypcji przekazywanego dostawcy silnika konwersacyjnego — **nie są redagowane przed przekazaniem** — podobnie jak tekst transkrypcji przekazywany funkcjom uruchamianym po rozmowie. **PESEL, data urodzenia i numer ubezpieczenia nie są w ogóle udostępniane modelowi.**
3. **Ocena skutków transferu.** Dla każdego transferu poza EOG Podmiot przetwarzający utrzymuje aktualną ocenę skutków transferu wraz ze standardowymi klauzulami umownymi i udostępnia je na żądanie w 7 dni. Niniejszy paragraf wraz z udostępnioną Listą podprocesorów stanowi udokumentowane polecenie Administratora w rozumieniu §13 ust. 1.

§20 Środki techniczne i organizacyjne (art. 32 RODO)

1. **Szyfrowanie i rezydencja.** Dane wrażliwe — szyfrowanie kopertowe AES-GCM-256, odrębny klucz dla każdego rekordu, związany kryptograficznie z placówką; klucz główny w zarządzanym magazynie kluczy szyfrujących (KMS). Transmisja — TLS. Hosting, baza danych, klucze, kopie zapasowe i nagrania — region UE (Warszawa), z odtwarzaniem punkt-w-czasie.
2. **Uczciwe zastrzeżenie.** Imię, nazwisko i numer telefonu pacjenta lub opiekuna są przechowywane jako **tekst jawny** — nie są szyfrowane polowo; chroni je izolacja danych placówki, granica uwierzytelniania i szyfrowanie dyskowe w spoczynku. Szyfrowanie polowe tych pól to zaplanowana migracja.
3. **Izolacja i dostęp.** Dane każdej placówki odseparowane na poziomie silnika bazy danych (Row-Level Security + FORCE RLS); hasła haszowane argon2id, klucze API jako skróty SHA-256, dostępne 2FA/TOTP; dostęp administracyjny wyłącznie przez warstwę kontroli dostępu dostawcy chmury (logowanie i drugi składnik), na kontach imiennych; **dziennik audytowy niezmienialny**.
4. **Minimalizacja i środowiska.** PESEL, data urodzenia i numer ubezpieczenia **nigdy** nie trafiają do modelu; funkcje zapisu klinicznego nie są dostępne asystentowi głosowemu; treść transkrypcji i nagrania widzą wyłącznie role Właściciel i Menedżer. Komponent wymiany danych z własnym oprogramowaniem Administratora (§12 ust. 2) działa na jego komputerze **wyłącznie w ruchu wychodzącym, bez zdalnego dostępu**. Rozdzielenie dev/prod, testy na danych syntetycznych, brak treningu modelu na danych pacjentów i klientów. AI wyłącznie asystuje.