

Polityka prywatności OtterSafe

wersja z dnia 4 października 2026 r. · obowiązuje od dnia 21 października 2026 r.

I. Administrator i kontakt

1. Administratorem danych osobowych związanych z Kontem i korzystaniem z OtterSafe jest OTTERS SAFE sp. z o.o. z siedzibą w Białymstoku, ul. Legionowa 10/208, 15-099 Białystok, wpisana do rejestru przedsiębiorców KRS pod numerem 0001259378, NIP 5423518362, REGON 545448862.
2. W sprawach dotyczących prywatności można skontaktować się pod adresem kontakt@ottersafe.pl.

II. Zakres danych i cele przetwarzania

Administrator może przetwarzać następujące kategorie danych:

- **Konto i uwierzytelnianie:** imię, nazwisko, adres e-mail, numer telefonu, dane profilu zawodowego (specjalizacja, numer zaświadczenia lub prawa wykonywania zawodu, nazwa gabinetu, miejscowość), zdjęcie profilowe, w tym adres zdjęcia z konta Google, identyfikator Konta, skróty haseł, informacje o uwierzytelnianiu dwuskładnikowym, historia logowania i dane przekazane przy logowaniu Google lub Apple, w tym adres e-mail przekazany przez Apple albo adres z usługi Ukryj mój adres e-mail;
- **umowa i korzystanie z usługi:** wybrany Plan, historia zmian Subskrypcji, zaakceptowane wersje dokumentów, ustawienia Konta, komunikacja dotycząca usługi oraz informacje o zgłoszeniach i reklamacjach;
- **rozliczenia:** dane nabywcy, adres, NIP, informacje o płatności, identyfikatory Stripe, a przy zakupach mobilnych – identyfikator tokenu zakupu nadany przez Apple albo token raportowania transakcji Google Play, identyfikatory transakcji, aplikacji i raportów, kwoty, waluta, daty oraz kraj opodatkowania, faktury, korekty i informacje KSeF;
- **dane techniczne i bezpieczeństwa:** adres IP, dane urządzenia i przeglądarki, znaczniki czasu, identyfikatory sesji, tokeny powiadomień push, identyfikatory techniczne powiadomień, logi błędów, zdarzenia bezpieczeństwa, używane funkcje oraz rozmiar przesyłanej zaszyfrowanej zawartości; dane o wydajności Aplikacji przesyłane z przeglądarki (metoda i ścieżka zapytania, status i czas odpowiedzi, bez treści zapytań); dane dołączane do zgłoszenia błędu (adres strony, informacje o przeglądarce); platforma i wersja aplikacji mobilnej;
- **kontakt i marketing:** adres e-mail oraz dane zawarte w korespondencji, nazwa profilu i treść kontaktu przez Instagram lub TikTok, a także informacja o udzieleniu lub cofnięciu zgody marketingowej.

Dane są przetwarzane w celu zawarcia i wykonania umowy, prowadzenia Konta, udostępniania funkcji Aplikacji, obsługi logowania, płatności, faktur, KSeF, komunikacji, przypomnień i powiadomień, reklamacji, bezpieczeństwa, zapobiegania nadużyciom, ustalania lub obrony roszczeń oraz – po uzyskaniu odrębnej zgody – wysyłania newslettera i informacji produktowych.

III. Podstawy prawne

- art. 6 ust. 1 lit. b RODO – zawarcie i wykonanie umowy oraz działania podejmowane przed jej zawarciem;
- art. 6 ust. 1 lit. c RODO – obowiązki podatkowe, rachunkowe, KSeF oraz inne obowiązki prawne;
- art. 6 ust. 1 lit. f RODO – bezpieczeństwo i niezawodność Aplikacji, zapobieganie nadużyciom, obsługa korespondencji, reklamacji, dochodzenie i obrona roszczeń oraz prowadzenie dokumentacji potwierdzającej wykonanie obowiązków. Podstawą raportowania transakcji mobilnych Apple i Google jest prawnie uzasadniony interes Administratora polegający na rozliczeniu opłat za dystrybucję Aplikacji i utrzymaniu możliwości oferowania płatności przez Stripe zgodnie z warunkami App Store oraz programu Google Play External Offers. Raportowanie obejmuje również odnowienia i zwroty;
- art. 6 ust. 1 lit. a RODO – dobrowolna zgoda na komunikację marketingową i produktową; zgodę można wycofać w dowolnym momencie bez wpływu na zgodność z prawem wcześniejszego przetwarzania.

Podanie danych wymaganych przy rejestracji i rozliczeniu jest dobrowolne, lecz niezbędne do utworzenia Konta, zawarcia umowy albo zakupu płatnego Planu. Dane marketingowe są dobrowolne.

IV. Dane Pacjentów/Klientów

W odniesieniu do danych Pacjentów/Klientów wprowadzanych przez Użytkownika administratorem jest co do zasady Użytkownik, a OtterSafe przetwarza te dane w jego imieniu jako podmiot przetwarzający. Zasady powierzenia określa § 10 Regulaminu.

Wybrane treści, w szczególności dane identyfikacyjne Pacjenta/Klienta, notatki, formularze i wybrane pola kliniczne, są szyfrowane na urządzeniu Użytkownika. OtterSafe może odczytywać metadane niezbędne do działania usługi, bezpieczeństwa i rozliczeń, w szczególności identyfikatory rekordów, daty i godziny, typy i statusy sesji, informacje o plikach i udostępnieniach, adresy e-mail odbiorców udostępnień i formularzy, linki do spotkań oraz zdarzenia audytowe. Szczegółowy zakres zależy od używanej funkcji.

Na polecenie Użytkownika OtterSafe wysyła e-mailem do wskazanych przez niego osób link do spotkania online (z imieniem i nazwiskiem Użytkownika, datą, godziną i czasem trwania sesji), linki do udostępnionych dokumentów lub linki do formularzy. Wiadomości są wysyłane za pośrednictwem OVH, a adres odbiorcy jest zapisywany w logach technicznych wysyłki. Osoba wypełniająca formularz widzi informację, że administratorem jej danych jest Użytkownik, który przesłał jej link.

Dalsze podmioty przetwarzające dane powierzone przez Użytkownika (§ 10 ust. 11 Regulaminu):

- **Microsoft Ireland Operations Limited (Microsoft Azure)** – hosting Aplikacji, bazy danych, plików i kopii zapasowych oraz logi techniczne; regiony Poland Central i North Europe;
- **OVH SAS** – wysyłka wiadomości e-mail do odbiorców wskazanych przez Użytkownika.

Dane powierzone nie są przekazywane poza Europejski Obszar Gospodarczy. Powiadomienia push wysyłane przez Google (Firebase Cloud Messaging) i Apple (APNs) nie zawierają danych Pacjentów/Klientów.

V. Okresy przechowywania

- **dane aktywnego Konta i dane aplikacyjne:** przez czas obowiązywania umowy; po zamknięciu Konta dane aplikacyjne i dane Pacjentów/Klientów są usuwane z aktywnych systemów, a powiązane pliki kierowane do bezpiecznego usunięcia;
- **minimalne dowody zawarcia i wykonania umowy, zgód oraz obsługi sporów:** do upływu właściwych terminów przedawnienia roszczeń lub zakończenia postępowania; zamknięte Konto jest w tym okresie zablokowane i zanonimizowane w zakresie danych niewymaganych do tego celu;
- **faktury, korekty i dane rozliczeniowe:** do upływu okresu wymaganego przez przepisy podatkowe i rachunkowe, co do zasady 5 lat od końca roku kalendarzowego, w którym upłynął termin płatności podatku, a dłużej, gdy bieg terminu został zawieszony lub przerwany;
- **dane telemetryczne w Azure Application Insights:** 90 dni;
- **pozostałe dane diagnostyczne w Azure Log Analytics:** domyślnie 30 dni, chyba że dla określonego typu danych skonfigurowano inny okres retencji; dane dotyczące konkretnego incydentu lub sporu mogą być przechowywane dłużej, wyłącznie w zakresie niezbędnym do jego wyjaśnienia albo ustalenia lub obrony roszczeń;
- **korespondencja:** co do zasady 12 miesięcy od zakończenia kontaktu, a w przypadku reklamacji, sporu lub obowiązku prawnego – przez okres niezbędny do ich obsługi i wykazania przebiegu sprawy;
- **dane marketingowe:** do czasu cofnięcia zgody albo stwierdzenia, że zgoda stała się nieaktualna;
- **udostępnienia dokumentów i formularzy, powiadomienia oraz tokeny powiadomień push:** do usunięcia przez Użytkownika albo do zamknięcia Konta; token push jest usuwany także po wylogowaniu na urządzeniu lub po zgłoszeniu przez Google albo Apple, że token jest nieaktualny;
- **tokeny zakupu i raportowania oraz dane o transakcjach zgłoszonych Apple i Google:** przez okres przechowywania faktur, korekt i danych rozliczeniowych, w zakresie potrzebnym do rozliczeń, korekt i wykazania prawidłowości raportowania;
- **dane u Stripe i Systim:** po zamknięciu Konta Administrator nie przekazuje im nowych danych; dane klienta, płatności i kontrahenta pozostają u tych dostawców przez okres wynikający z przepisów podatkowych i rachunkowych oraz ich własnych zasad przechowywania.

Kopie zapasowe danych przechowywanych w bazie Azure SQL są objęte mechanizmem Point-in-Time Restore (PITR) i przechowywane przez 7 dni. Administrator nie stosuje długoterminowej retencji tych kopii (Long-Term Retention, LTR). Kopie nie są wykorzystywane do zwykłego świadczenia usługi po zamknięciu Konta. Jeżeli baza musi zostać odtworzona po awarii, dane przeznaczone wcześniej do usunięcia podlegają ponownemu usunięciu.

W Azure Blob Storage jest włączony mechanizm soft delete dla blobów i kontenerów z okresem retencji 7 dni. Oznacza to, że usunięte pliki lub kontenery mogą być możliwe do odzyskania przez ten okres. Wersjonowanie blobów, Point-in-Time Restore oraz Azure Backup dla blobów są wyłączone.

VI. Odbiorcy danych

Dane mogą być przekazywane następującym odbiorcom w zakresie niezbędnym do realizacji ich zadań:

- **Microsoft Ireland Operations Limited (Microsoft Azure)** – hosting Aplikacji, bazy danych, plików, kopii zapasowych oraz Azure Application Insights i Log Analytics; podstawowa infrastruktura znajduje się w regionach Poland Central i North Europe;
- **OVH SAS** – poczta systemowa i marketingowa domeny ottersafe.pl, w tym wiadomości wysyłane na polecenie Użytkownika do Pacjentów/Klientów;
- **Google** – logowanie i weryfikacja tożsamości osób korzystających z logowania Google oraz usługa Firebase Cloud Messaging służąca do dostarczania powiadomień push. W ramach wysyłki powiadomienia Google otrzymuje token urządzenia, techniczny identyfikator powiadomienia, adres ekranu docelowego i ogólną treść komunikatu. Komunikat nie zawiera danych Pacjenta/Klienta ani szczegółów zdarzenia;
- **Apple** – logowanie i weryfikacja tożsamości osób korzystających z funkcji „Zaloguj się przez Apple” oraz Apple Push Notification service (APNs), wykorzystywana na urządzeniach Apple do dostarczania powiadomień push. W zależności od wyboru Użytkownika Apple może przekazać adres e-mail albo adres z usługi Ukryj mój adres e-mail. APNs otrzymuje token urządzenia i ogólną treść komunikatu; komunikat nie zawiera danych Pacjenta/Klienta ani szczegółów zdarzenia. Przy zakupie lub zmianie Planu w aplikacji iOS Apple wyświetla informację o płatności realizowanej przez Usługodawcę i nadaje identyfikator tokenu zakupu. Administrator przekazuje Apple ten identyfikator oraz dane transakcji powiązanych z Subskrypcją (rodzaj zdarzenia – zakup, odnowienie, zmiana Planu, zwrot; daty i okres Subskrypcji; Plan; kwoty netto, VAT i brutto; walutę i kraj opodatkowania) w celu rozliczenia prowizji Apple. Apple nie otrzymuje imienia, nazwiska, adresu e-mail, danych rozliczeniowych ani danych Pacjentów/Klientów i przetwarza te dane jako niezależny administrator;
- **Google (Google Play)** – sprawdzenie dostępności zakupów zewnętrznych na Androidzie, przekazanie tokenu raportowania i obsługa wymaganej informacji przed przejściem do Stripe. Administrator przekazuje Google token, identyfikatory transakcji i powiązania odnowień, identyfikator aplikacji, kwoty netto i podatku, walutę, daty, kraj opodatkowania oraz informacje o zwrotach w celu rozliczenia programu External Offers. W ramach tych raportów Administrator nie przekazuje Google imienia, nazwiska, adresu e-mail, pełnego adresu rozliczeniowego, danych karty ani danych Pacjentów/Klientów. Google przetwarza otrzymane dane jako niezależny administrator;
- **Stripe** – obsługa płatności, Subskrypcji i przeciwdziałanie oszustwom płatniczym; Stripe działa również jako niezależny administrator w zakresie określonym przez jego dokumentację;
- **System** – wystawianie, przechowywanie i obsługa faktur oraz przekazywanie dokumentów do KSeF;
- **biuro rachunkowe** – dostęp do danych rozliczeniowych i faktur za pośrednictwem System;
- **Szef Krajowej Administracji Skarbowej i inne uprawnione organy** – dane faktur przekazywane przez KSeF lub na podstawie obowiązujących przepisów;
- **Meta Platforms Ireland Limited i TikTok Technology Limited** – dane związane z kontaktem przez Instagram lub TikTok, zgodnie z zasadami tych serwisów;
- doradcy prawni, audytorzy i inne podmioty wspierające Administratora, jeżeli jest to niezbędne i posiadają właściwe upoważnienie lub podstawę prawną.

Administrator nie wpisuje do niniejszej listy dostawców planowanych, lecz jeszcze nieużywanych produkcyjnie. Przed uruchomieniem nowego dostawcy, któremu mają być przekazywane dane, dokument zostanie odpowiednio zaktualizowany.

VII. Przekazywanie danych poza EOG

Podstawowa infrastruktura Aplikacji jest utrzymywana w Unii Europejskiej. W związku z korzystaniem z globalnych usług Google, Apple, Stripe, Meta lub TikTok niektóre dane mogą być przetwarzane poza Europejskim Obszarem Gospodarczym. W takim przypadku przekazanie odbywa się na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, standardowych klauzul umownych lub innego mechanizmu przewidzianego w rozdziale V RODO, wraz z dodatkowymi zabezpieczeniami, gdy są wymagane. Informację o właściwym mechanizmie dla konkretnego dostawcy można uzyskać pod adresem kontakt@ottersafe.pl.

VIII. Prawa osób

W granicach wynikających z RODO osobie, której dane dotyczą, przysługuje prawo dostępu do danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu oraz cofnięcia zgody. Żądanie można przesłać na adres kontakt@ottersafe.pl. Przysługuje również prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Dane nie są wykorzystywane do zautomatyzowanego podejmowania decyzji wywołujących skutki prawne lub podobnie istotnie wpływających na osobę ani do profilowania w rozumieniu art. 22 RODO.

IX. Pliki cookies, pamięć urządzenia i aplikacje mobilne

OtterSafe wykorzystuje techniczne pliki cookies oraz podobne mechanizmy pamięci przeglądarki (localStorage, sessionStorage, IndexedDB) wyłącznie do utrzymania sesji, bezpieczeństwa logowania, szyfrowania po stronie urządzenia, przechowywania zaszyfrowanych szkiców niezapisanych notatek, obsługi powiadomień push oraz zapamiętania ustawień interfejsu, np. zamkniętych komunikatów. Klucz szyfrowania odblokowany w przeglądarce jest przechowywany tylko do końca sesji przeglądarki. Nie są używane Google Analytics, Meta Pixel, Hotjar ani podobne narzędzia marketingowe lub analityczne. Mechanizmy te są niezbędne do świadczenia usługi i nie wymagają odrębnej zgody.

Aplikacje mobilne dla iOS i Android wyświetlają wersję internetową Aplikacji i dodatkowo:

- po zgodzie Użytkownika przekazują Administratorowi token powiadomień push wraz z platformą i wersją aplikacji;
- po włączeniu odblokowania biometrycznego przechowują klucz szyfrowania w systemowym magazynie kluczy urządzenia (iOS Keychain albo Android Keystore). Weryfikację biometryczną wykonuje system operacyjny; Administrator nie otrzymuje ani nie przetwarza danych biometrycznych;
- w aplikacji iOS, przed przejściem do płatności, pobierają z systemu identyfikator tokenu zakupu Apple i przekazują go Administratorowi;
- w aplikacji Android sprawdzają dostępność External Offers, pobierają z Google Play token raportowania transakcji i przekazują go Administratorowi wraz z identyfikatorem aplikacji; po potwierdzeniu wymaganych informacji otwierają stronę płatności Stripe w przeglądarce;
- przechowują lokalnie liczniki uruchomień, aby w odpowiednim momencie wyświetlić systemową prośbę o ocenę aplikacji (Apple App Store albo Google Play). Wystawienie oceny odbywa się na zasadach sklepu;
- proszą o dostęp do aparatu, mikrofonu lub zapisu zdjęć (iOS) tylko wtedy, gdy Użytkownik chce dodać albo zapisać plik;

- nie zawierają narzędzi analitycznych, reklamowych ani śledzących i nie używają identyfikatora reklamowego.

Pliki pobrane z aplikacji na urządzenie, na Androidzie zapisywane w folderze pobranych plików, nie są chronione szyfrowaniem OtterSafe. Pliki otwierane tylko do podglądu są usuwane z pamięci podręcznej po zamknięciu podglądu.

X. Zmiany polityki

O istotnych zmianach Polityki prywatności Administrator informuje e-mailem z odpowiednim wyprzedzeniem, wskazując zakres i datę wejścia zmian w życie. Poprzednie wersje pozostają dostępne w archiwum na stronie OtterSafe.