FLEXCLOUD

Polityka prywatności FlexCloud

Wersja: 2.0
Data obowiązywania: 28 lipca 2026
Data publikacji: —
Język / Language: PL

SHA-256
fd0d32a47f9bee1fb9fc1e6c399297e6ad31912320b88033112c95f2fa65232d

Spis treści

1. POLITYKA PRYWATNOŚCI FLEXCLOUD

2. 1. Administrator danych

Administratorem danych osobowych jest FlexCloud Dawid Majer, przedsiębiorca prowadzący jednoosobową działalność gospodarczą wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP 5922306106, REGON 542529330, adres: ul. Heleny Lange 14, 83-200 Starogard Gdański, serwis: https://flexcloud.pl, e-mail: bok@flexcloud.pl, tel.: +48784173386. Kontakt w sprawach danych osobowych: bok@flexcloud.pl z tytułem „RODO”.

3. 2. Zakres danych

FlexCloud może przetwarzać w szczególności: imię i nazwisko, firmę, NIP, REGON, adres, e-mail, telefon, identyfikatory konta i usług, dane zamówień i płatności, historię kontaktu i zgłoszeń, adresy IP, identyfikatory urządzeń, logi bezpieczeństwa, dane techniczne serwerów, informacje o zgodach i wersjach dokumentów, dane wynikające ze zgłoszeń nadużyć oraz dane wymagane do wystawienia dokumentów księgowych.

4. 3. Cele i podstawy przetwarzania

1. Zawarcie i wykonanie Umowy, prowadzenie konta, aktywacja, odnowienia, obsługa płatności i wsparcie – niezbędność do wykonania Umowy lub podjęcia działań przed jej zawarciem.

2. Wystawianie dokumentów księgowych, rozliczenia podatkowe, obowiązki rachunkowe i realizacja żądań organów – obowiązek prawny.

3. Bezpieczeństwo infrastruktury, zapobieganie oszustwom, ochrona przed nadużyciami, dochodzenie i obrona roszczeń, prowadzenie audytu, tworzenie kopii operacyjnych i zapewnienie ciągłości – prawnie uzasadniony interes FlexCloud.

4. Marketing elektroniczny, newsletter oraz niekonieczne cookies lub podobne technologie – zgoda, jeżeli jest wymagana.

5. Obsługa zgłoszeń treści nielegalnych i nadużyć – obowiązek prawny oraz prawnie uzasadniony interes polegający na ochronie użytkowników i infrastruktury.

5. 4. Dobrowolność danych

Podanie danych potrzebnych do zawarcia i wykonania Umowy jest dobrowolne, ale konieczne do realizacji zamówienia. Podanie danych do marketingu jest dobrowolne i nie wpływa na możliwość zakupu Usługi.

6. 5. Odbiorcy danych

Dane mogą być przekazywane podmiotom świadczącym na rzecz FlexCloud usługi: płatnicze, bankowe, księgowe, hostingowe, chmurowe, pocztowe, wsparcia, bezpieczeństwa, monitoringu, obsługi prawnej, odzyskiwania należności, fakturowania i KSeF. Zakres danych jest ograniczany do niezbędnego minimum. Operatorzy płatności mogą działać jako odrębni administratorzy zgodnie z własnymi obowiązkami prawnymi.

7. 6. Transfery poza EOG

Jeżeli dostawca narzędzia przetwarza dane poza Europejskim Obszarem Gospodarczym, FlexCloud stosuje podstawy i zabezpieczenia wymagane przez RODO, w szczególności decyzję stwierdzającą odpowiedni stopień ochrony albo standardowe klauzule umowne, o ile mają zastosowanie.

8. 7. Okres przechowywania

1. Dane konta i Umowy – przez czas świadczenia Usługi, a następnie przez okres potrzebny do rozliczeń, obrony roszczeń i wykonania obowiązków prawnych.

2. Dokumenty księgowe – przez okres wymagany przepisami podatkowymi i rachunkowymi.

3. Zgłoszenia i korespondencja – co do zasady do 36 miesięcy od zakończenia sprawy, dłużej, jeżeli jest to konieczne dla roszczeń lub obowiązków prawnych.

4. Logi bezpieczeństwa i dostępu – co do zasady do 12 miesięcy, chyba że incydent, postępowanie lub prawo uzasadnia dłuższe przechowywanie.

5. Dane sandbox/test – do zakończenia testu i okresu potrzebnego do audytu, nie dłużej niż jest to konieczne; nie powinny zawierać danych prawdziwych klientów poza kontrolowanymi kontami testowymi.

6. Dane marketingowe – do wycofania zgody lub skutecznego sprzeciwu.

9. 8. Prawa osób

Osobie przysługuje – zależnie od podstawy i okoliczności – prawo dostępu, sprostowania, usunięcia, ograniczenia, przenoszenia, sprzeciwu, wycofania zgody oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Wycofanie zgody nie wpływa na zgodność wcześniejszego przetwarzania.

10. 9. Zautomatyzowane decyzje

FlexCloud może stosować automatyczne reguły bezpieczeństwa, np. czasowe blokowanie nietypowych logowań lub płatności. Jeżeli decyzja wywołuje skutek prawny lub podobnie istotny wyłącznie w sposób zautomatyzowany, FlexCloud zapewnia informacje i prawa wymagane przez RODO. Ostateczna decyzja o trwałym rozwiązaniu Umowy z powodu oszustwa powinna podlegać weryfikacji człowieka, chyba że natychmiastowe działanie jest konieczne dla bezpieczeństwa.

11. 10. Bezpieczeństwo

FlexCloud stosuje środki techniczne i organizacyjne odpowiednie do ryzyka, w szczególności kontrolę dostępu, szyfrowanie transmisji, rejestrowanie operacji administracyjnych, kopie operacyjne, rozdzielenie środowisk oraz procedury reagowania na incydenty.

12. 11. Cookies i technologie podobne

Szczegółowe zasady określa Polityka cookies. Niekonieczne technologie są uruchamiane dopiero po uzyskaniu ważnej zgody, jeżeli zgoda jest wymagana. Użytkownik może zmienić lub wycofać wybór równie łatwo, jak go udzielił.

13. 12. Zmiany Polityki

Polityka może zostać zmieniona w związku ze zmianami prawa, dostawców, funkcji Serwisu lub procesów przetwarzania. Aktualna wersja, data wejścia w życie i suma kontrolna są publikowane w rejestrze dokumentów FlexCloud.

14. 13. Telefonia i system IVR

1. W związku z obsługą numeru kontaktowego FlexCloud może przetwarzać metadane rozmowy: skrócony lub zahashowany numer dzwoniącego, identyfikator połączenia, wybraną kategorię, datę, czas trwania, status autoryzacji, identyfikator klienta, powiązaną usługę i numer utworzonego

zgłoszenia.

2. Weryfikacja osoby dzwoniącej może obejmować podanie ID klienta albo numeru telefonu przypisanego do konta oraz jednorazowego kodu przekazanego do panelu klienta lub zweryfikowanego kanału kontaktowego. Kod jest krótkotrwały, jednorazowy i przechowywany wyłącznie w postaci skrótu kryptograficznego.

3. System nie nagrywa treści rozmów w konfiguracji domyślnej. Włączenie nagrywania wymaga osobnego komunikatu przed rozpoczęciem nagrania, określenia celu, podstawy, czasu retencji i aktualizacji niniejszej Polityki.

4. Metadane nieudanych, niepowiązanych z klientem prób są usuwane lub anonimizowane po okresie niezbędnym dla bezpieczeństwa i diagnostyki. Dane rozmów powiązanych ze zgłoszeniem są przechowywane zgodnie z okresem retencji danego zgłoszenia i obowiązkami związanymi z ochroną roszczeń.

5. Bezpośrednie przekazanie rozmowy do administratora dyżurnego jest ograniczone do zweryfikowanych spraw krytycznych, w szczególności aktywnej awarii, zagrożenia bezpieczeństwa, ryzyka utraty danych albo pilnej sprawy dotyczącej aktywnego projektu.