POLITYKA PRYWATNOŚCI (PP)

Dla platformy/strony/serwisu/usług znajdującego/znajdujących się pod adresem domeny " voxihost.pl"

Niniejszy dokument jest częścią zbioru dokumentów:

a. Regulamin Usług (TOS)
b. Polityka Prywatności (PP)
c. Umowa o Gwarantowanym Poziomie Świadczenia Usług (SLA)
d. Polityka Uczciwego Korzystania (FUP)

Data Wprowadzenia: 14.02.2026

Data Aktualizacji: 15.01.2026

§ 1. POSTANOWIENIA WSTĘPNE I DEFINICJE

1.1. Administrator Danych Osobowych:

a. VoxiHost DANIEL MARSZAŁKOWSKI
b. ul. 3 Maja 29, 62-500 Konin, Polska
c. **NIP:** 6653080651 | REGON: 542936383
d. **E-mail:** support@voxihost.pl

(dalej zwany "VoxiHost" lub "Operatorem").

1.2. Zakres Obowiązywania: Niniejsza Polityka Prywatności stanowi integralną część Regulaminu Usług i obowiązuje wyłącznie w ramach serwisu internetowego dostępnego pod domeną VoxiHost.pl. Dokument ten nie ma zastosowania do innych serwisów, projektów czy stron internetowych prowadzonych przez Operatora pod innymi adresami.

1.3. Cel: Celem niniejszej Polityki Prywatności jest zapewnienie transparentności w zakresie przetwarzania danych osobowych oraz realizacja obowiązków informacyjnych wynikających z RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.).

1.4. Akceptacja: Rejestracja Konta lub zamówienie Usługi jest równoznaczne z pełną akceptacją niniejszego dokumentu oraz wszystkich dokumentów powiązanych. W przypadku wprowadzenia zmian w Polityce Prywatności, Klient zostanie poinformowany zgodnie z §12.2. Brak sprzeciwu w terminie 30 dni od powiadomienia oznacza akceptację zmian. Klient ma prawo wypowiedzieć umowę w przypadku braku akceptacji zmian.

§ 2. JAKIE DANE ZBIERAMY

Niniejsza polityka dotyczy danych, których jesteś właścicielem (Dane Konta). W przypadku danych, które przechowujesz w ramach Usług Cyfrowych (pliki, bazy danych, aplikacje), Operator działa jedynie jako Podmiot Przetwarzający (Procesor) udostępniający infrastrukturę. Nie ingerujemy w te treści, nie analizujemy ich ani nie udostępniamy, chyba że na wyraźny nakaz sądu lub prokuratury.

2.1. Dane Tożsamości: Imię, nazwisko, wiek (data urodzenia), nazwa firmy, NIP, adres zamieszkania/siedziby.

2.2. Dane Kontaktowe: Adres e-mail, numer telefonu (do powiadomień SMS/2FA).

2.3. Dane Techniczne (Device Fingerprint): Adres IP, typ przeglądarki (User-Agent), rozdzielczość ekranu, strefa czasowa, system operacyjny - używane do tworzenia "odcisku palca" urządzenia w

celu wykrywania multikont i oszustw.

2.4. Dane Finansowe: Historia transakcji, metoda płatności, identyfikatory transakcji (Transaction ID). Nie przechowujemy pełnych numerów kart płatniczych (są one procesowane bezpośrednio przez zewnętrznego Operatora Płatności).

2.5. Dane Weryfikacyjne (KYC): Status weryfikacji, skrót (hash) dokumentu tożsamości, wynik oceny wiarygodności (Scoring).

2.6. Logi Serwerowe i Telemetria Bezpieczeństwa: Historia logowań, pełne logi aktywności w Panelu (Audit Log), a także zanonimizowane metadane ruchu sieciowego (NetFlow/sFlow) analizowane w czasie rzeczywistym w celu wykrywania anomalii i cyberataków.

2.7. Weryfikacja Tożsamości (KYC) i DiDit.me:

a. Weryfikacja tożsamości (KYC) jest przeprowadzana przez zewnętrzny podmiot **DiDit.me**, który jest niezależnym administratorem danych osobowych.

b. Operator jest odrębnym administratorem w zakresie przetwarzania wyniku weryfikacji.

c. Szczegółowy opis procesu KYC, w tym zakresu danych i okresów przechowywania, znajduje się w Regulaminie Usług (TOS §3.4).

d. **Podstawa prawna:** Art. 6 ust. 1 lit. b RODO (wykonanie umowy).

§ 3. CELE I PODSTAWY PRAWNE PRZETWARZANIA

Ilekroć w poniższej sekcji mowa o RODO, rozumie się przez to 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.

3.1. Świadczenie Usług:

a. **Podstawa:** Art. 6 ust. 1 lit. b RODO.

b. **Wyjaśnienie:** Niezbędne do wykonania umowy (świadczenie Usług, dostęp do Panelu Klienta).

3.2. Obsługa Płatności:

a. **Podstawa:** Art. 6 ust. 1 lit. b RODO.

b. **Wyjaśnienie:** Procesowanie doładowań vPLN i wystawianie faktur.

3.3. Marketing Własny:

a. **Podstawa dla przetwarzania danych:** Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes).

b. **Podstawa dla komunikacji elektronicznej:** Art. 6 ust. 1 lit. a RODO (zgoda) - wymagana zgodnie z Prawem Komunikacji Elektronicznej (PKE Art. 398, obowiązujące od 10.11.2024).

c. **Wyjaśnienie:** Możemy przetwarzać Twoje dane kontaktowe w celach marketingowych (informowanie o nowościach, promocjach, rozwoju usług). **Wysyłka wiadomości e-mail lub SMS marketingowych wymaga Twojej odrębnej zgody.** Zgodę możesz wycofać w każdej chwili poprzez kliknięcie linku "wypisz się" w wiadomości lub kontakt z support@voxihost.pl.

d. **Mechanizm wyrażania zgody:** Zgoda na marketing elektroniczny wyrażana jest poprzez zaznaczenie opcjonalnego pola podczas rejestracji lub w późniejszym czasie w Panelu Klienta. Pole jest domyślnie niezaznaczone - zgoda nie jest wymagana do założenia konta. Zgodę można wycofać w każdej chwili.

3.4. Obowiązki Podatkowe:

a. **Podstawa:** Art. 6 ust. 1 lit. c RODO.

b. **Wyjaśnienie:** Przechowywanie faktur przez 5 lat (wymóg ustawy o rachunkowości).

3.5. Bezpieczeństwo i Logi:

a. **Podstawa:** Art. 6 ust. 1 lit. f RODO.

b. **Wyjaśnienie:** Prawnie uzasadniony interes: obrona przed DDoS, włamaniami i Abuse.

3.6. Ocena Ryzyka (Anti-Fraud):

a. **Podstawa:** Art. 6 ust. 1 lit. f RODO.

b. **Wyjaśnienie:** Prawnie uzasadniony interes: weryfikacja zagrożeń, zapobieganie wyłudzeniom.

3.7. Obsługa Zgłoszeń Abuse:

a. **Podstawa:** Art. 6 ust. 1 lit. f RODO.

b. **Wyjaśnienie:** Przetwarzanie danych osób zgłaszających naruszenia (sygnalistów) w celu analizy i reakcji na incydenty.

3.8. Dochodzenie Roszczeń:

a. **Podstawa:** Art. 6 ust. 1 lit. f RODO.

b. **Wyjaśnienie:** Windykacja należności, obrona przed chargebackami.

3.9. Dobrowolność Podania Danych: Podanie danych osobowych jest dobrowolne, jednakże jest warunkiem niezbędnym do zawarcia umowy. Konsekwencją niepodania danych będzie brak możliwości założenia konta i korzystania z Usług.

§ 4. PROFILOWANIE I ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

W trosce o bezpieczeństwo infrastruktury stosujemy systemy zautomatyzowane (profilowanie), które oceniają wiarygodność Klienta.

4.1. Na Czym Polega: System analizuje adres IP, fingerprint urządzenia, kraj pochodzenia, historię płatności oraz weryfikuje obecność danych w zewnętrznych bazach zagrożeń i rejestrach nadużyć (Threat Intelligence/RBL).

4.2. Skutek: Jeśli system wykryje wysokie ryzyko (np. IP powiązane z botnetem, kradziona karta), rejestracja może zostać automatycznie odrzucona lub usługa zablokowana.

4.3. Twoje Prawa: Masz prawo do uzyskania interwencji ludzkiej. Jeśli uważasz, że system pomylił się, napisz do nas na adres support@voxihost.pl - pracownik zweryfikuje decyzję ręcznie.

§ 5. ODBIORCY DANYCH (PROCESORZY)

Twoje dane przekazujemy tylko zaufanym podmiotom, które pomagają nam świadczyć usługi (Procesorzy). Zamiast wymieniać każdą firmę z nazwy, wskazujemy kategorie odbiorców (zgodnie z RODO):

5.1. Infrastruktura i Bezpieczeństwo:

a. Dostawcy usług Data Center i kolokacji (zlokalizowani w EOG).

b. Dostawcy usług sieciowych, CDN (Content Delivery Network) oraz zabezpieczeń przed atakami DDoS i WAF (Web Application Firewall).

5.2. Płatności: Operatorzy płatności elektronicznych i banki (np. Stripe, PayPal) - w zakresie niezbędnym do realizacji transakcji.

5.3. Wsparcie i Weryfikacja: Dostawcy systemów weryfikacji tożsamości (Identity Verification) - w celu przeciwdziałania wyłudzeniom.

5.4. Obsługa Administracyjna:

a. Biuro rachunkowe / Dostawcy systemów księgowych.
b. Kancelarie prawne i firmy windykacyjne (wyłącznie w przypadku dochodzenia roszczeń).

§ 6. TRANSFERY POZA EOG

Współpracujemy z dostawcami usług (np. w zakresie bezpieczeństwa sieciowego czy płatności), którzy mogą przetwarzać dane w USA. Transfer ten jest bezpieczny i zgodny z prawem na podstawie:

6.1. Data Privacy Framework (DPF): Decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony danych w USA.

6.2. Standardowe Klauzule Umowne (SCC): Dodatkowe zabezpieczenia prawne w umowach z dostawcami.

6.3. Przekazywanie Danych Organom Poza EOG: W wyjątkowych przypadkach, gdy otrzymamy prawnie wiążące żądanie ujawnienia danych osobowych od organu publicznego państwa spoza EOG (np. wniosek o pomoc prawną od organów ścigania), przekazanie nastąpi wyłącznie jeśli żądanie:

a. jest zgodne z umową międzynarodową (np. konwencja o wzajemnej pomocy prawnej),
b. dotyczy konkretnego przypadku i nie ma charakteru masowego,
c. zostało zweryfikowane pod kątem zgodności z prawem UE przez prawnika.

Operator informuje UODO o każdym takim żądaniu, chyba że jest to zabronione (np. tajemnica śledztwa).

§ 7. BEZPIECZEŃSTWO DANYCH

Stosujemy środki techniczne i organizacyjne zgodne ze standardami branżowymi:

7.1. Szyfrowanie: Wszystkie połączenia (HTTP/API) są szyfrowane protokołem TLS 1.3. Bazy danych i dyski są szyfrowane w spoczynku (AES-256).

7.2. Hashing Haseł: Hasła użytkowników są hashowane silnym algorytmem (Argon2/Bcrypt) i nigdy nie są przechowywane tekstem jawnym.

7.3. Minimalizacja Dostępu: Dostęp do danych mają tylko upoważnieni pracownicy (zasada need-to-know), zabezpieczeni uwierzytelnianiem dwuskładnikowym (2FA).

7.4. Backupy: Kopie zapasowe systemów administracyjnych Operatora (bazy danych kont, panel klienta) są szyfrowane i przechowywane w oddzielnej lokalizacji geograficznej. Uwaga: Powyższe nie dotyczy kopii zapasowych danych wewnątrz serwera VPS Klienta, za które odpowiada sam Klient (zgodnie z Regulaminem).

7.5. Procedura Naruszeń: W przypadku wykrycia naruszenia ochrony danych osobowych (Data Breach), które może powodować ryzyko naruszenia praw użytkowników, zgłosimy incydent do Prezesa UODO w ciągu **72 godzin** od jego wykrycia (zgodnie z art. 33 RODO). W przypadku wysokiego ryzyka, poinformujemy również osoby, których dane dotyczą, bez zbędnej zwłoki (zgodnie z art. 34 RODO).

7.6. Testy Bezpieczeństwa: Operator przeprowadza regularne audyty bezpieczeństwa infrastruktury, w tym testy penetracyjne (pentesty) oraz przeglądy kodu (code review) w celu identyfikacji i usuwania luk w zabezpieczeniach.

§ 8. OKRES RETENCJI (JAK DŁUGO TRZYMAMY DANE)

8.1. Dane Konta: Przez okres trwania umowy + **30 dni** po jej rozwiązaniu (bufor na pomyłki).

8.2. Faktury: 5 lat od początku roku następującego po roku podatkowym (wymóg prawny - ustawa o

rachunkowości, Art. 74 ust. 3).

8.3. Logi Techniczne: Przez okres **12 miesięcy** (lub inny okres wymagany przez obowiązujące przepisy Prawa Komunikacji Elektronicznej - PKE, Art. 47) w celach bezpieczeństwa i na żądanie uprawnionych organów.

8.4. Retencja Danych w Celach Bezpieczeństwa (Ochrona przed Recydywą):

a. W przypadku Klientów zablokowanych za poważne naruszenie Regulaminu (Abuse, Fraud, Ataki na infrastrukturę), Operator zachowuje prawo do przechowywania ich danych (w tym: adres IP, fingerprint, dowody naruszenia, korespondencja) przez okres **10 lat** od daty zablokowania konta, w oparciu o Prawnie Uzasadniony Interes Administratora (Art. 6 ust. 1 lit. f RODO).

b. Operator może również przechowywać zanonimizowane dane weryfikacyjne (np. hash kryptograficzny dokumentu tożsamości) przez okres do **10 lat** w celu zapobiegania ponownej rejestracji osób dopuszczających się poważnych naruszeń.

c. Celem jest obrona przed roszczeniami, zabezpieczenie infrastruktury oraz zabezpieczenie materiału dowodowego dla organów ścigania.

d. W tym zakresie prawo do usunięcia danych jest ograniczone. Po upływie okresu retencji (10 lat), dane są automatycznie usuwane, chyba że zachowanie danych jest niezbędne do obrony przed toczącym się postępowaniem sądowym lub karnym.

e. **Wyjątek dla Amnestii:** W przypadku, gdy Klient pomyślnie przeszedł procedurę Amnestii (zgodnie z Regulaminem Usług) i nie dopuścił się ponownego naruszenia przez okres minimum 2 lat od odblokowania usługi, dane z pierwotnego naruszenia mogą zostać usunięte na wniosek Klienta. Decyzję podejmuje Operator po weryfikacji braku nowych incydentów.

8.5. Automatyczne Usuwanie: Po upływie okresów retencji określonych w §8.1-8.4, dane są automatycznie usuwane z systemów produkcyjnych i kopii zapasowych zgodnie z procedurami bezpieczeństwa (overwrite/shredding), uniemożliwiającymi ich odzyskanie.

§ 9. TWOJE PRAWA I ICH OGRANICZENIA

Przysługuje Ci prawo do:

9.1. Dostępu do Swoich Danych: Możesz poprosić o kopię przechowywanych przez nas danych osobowych.

9.2. Sprostowania Danych: Możesz poprosić o korektę nieprawidłowych lub niekompletnych danych.

9.3. Usunięcia Danych ("Prawo do Bycia Zapomnianym"): Z zastrzeżeniem, że prawo to nie przysługuje, jeżeli przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń (np. jeśli masz nieopłacone faktury lub zostałeś zbanowany za naruszenie Regulaminu).

9.4. Ograniczenia Przetwarzania: Możesz poprosić o tymczasowe wstrzymanie przetwarzania danych w określonych przypadkach.

9.5. Przenoszenia Danych: Możesz poprosić o otrzymanie danych w ustrukturyzowanym, powszechnie używanym formacie (np. JSON).

9.6. Sprzeciwu: Masz prawo wnieść sprzeciw wobec przetwarzania danych na podstawie prawnie uzasadnionego interesu. Operator może go odrzucić, jeśli wykaże istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec Twoich interesów (np. bezpieczeństwo całej sieci Operatora).

9.7. Wniesienia Skargi: Masz prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (UODO), ul. Stanisława Moniuszki 1A, 00-014 Warszawa.

9.8. Składanie Wniosków: Wnioski dotyczące realizacji powyższych praw prosimy kierować na adres: support@voxihost.pl. Odpowiemy w ciągu **1 miesiąca** od otrzymania wniosku (zgodnie z

art. 12.3 RODO). W uzasadnionych przypadkach (np. złożoność żądania, duża liczba wniosków) możemy przedłużyć ten termin o kolejne 2 miesiące, informując Cię o przyczynach opóźnienia.

§ 10. OCHRONA DZIECI

Nasze usługi są skierowane wyłącznie do osób, które ukończyły **16 lat** (zgodnie z Regulaminem). Nie zbieramy świadomie danych osobowych od dzieci. W przypadku wykrycia, że konto zostało założone przez osobę poniżej tego wieku bez zgody opiekuna prawnego, podejmiemy kroki w celu natychmiastowego usunięcia takich danych i blokady konta.

§ 11. PLIKI COOKIES I LOCAL STORAGE

Strona używa plików cookies oraz pamięci lokalnej przeglądarki (Local Storage) w minimalnym zakresie:

11.1. Niezbędne (Techniczne): Utrzymanie sesji zalogowania, zapamiętanie preferencji (np. motyw jasny/ciemny), zapobieganie atakom CSRF.

11.2. Bezpieczeństwo (Cloudflare/Turnstile): Wykrywanie botów (rozróżnianie ludzi od automatów).

11.3. Brak Cookies Śledzących: Nie stosujemy cookies marketingowych ani śledzących podmiotów trzecich (np. Google Analytics, Facebook Pixel). Szanujemy Twoją prywatność.

§ 12. ZMIANY POLITYKI PRYWATNOŚCI

12.1. Prawo do Zmian: Operator zastrzega sobie prawo do wprowadzania zmian w niniejszej Polityce Prywatności w przypadku zmiany przepisów prawa, technologii lub sposobów przetwarzania danych.

12.2. Powiadomienie o Zmianach: O każdej istotnej zmianie poinformujemy Klienta drogą mailową lub poprzez komunikat w Panelu Klienta z wyprzedzeniem co najmniej **30 dni**. Brak sprzeciwu w terminie **30 dni** od powiadomienia oznacza akceptację zmian. W przypadku sprzeciwu, Klient ma prawo wypowiedzieć umowę zgodnie z postanowieniami TOS.

12.3. Dostępność: Aktualna wersja Polityki Prywatności jest zawsze dostępna na stronie VoxiHost.pl w stopce strony oraz w Panelu Klienta po zalogowaniu, w formie umożliwiającej pobranie, utrwalenie i wydrukowanie. Data ostatniej aktualizacji znajduje się w nagłówku dokumentu.