TRANSLATION NOTICE

This document has been automatically translated from Polish to English using artificial intelligence for informational purposes only.

In the event of any discrepancies, inconsistencies, or conflicts between the English and Polish language versions of this document, **the Polish language version shall prevail and constitute the sole legally binding version**.

For official and legally binding information, users are advised to consult the original Polish language document.

Users who do not understand Polish are advised to seek independent legal advice before accepting these terms.

PRIVACY POLICY (PP)

For the platform/website/service/services located at the domain address " voxihost.pl"

This document is part of a set of documents:

a. Terms of Service (TOS)
b. Privacy Policy (PP)
c. Service Level Agreement (SLA)
d. Fair Usage Policy (FUP)

Effective Date: 14.02.2026

Last Updated: 15.01.2026

§ 1. INTRODUCTORY PROVISIONS AND DEFINITIONS

1.1. Personal Data Controller:

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

(hereinafter referred to as "VoxiHost" or the "Operator").

1.2. Scope of Application: This Privacy Policy constitutes an integral part of the Terms of Service and applies exclusively within the internet service available under the VoxiHost.pl domain. This document does not apply to other services, projects, or websites operated by the Operator under different addresses.

1.3. Purpose: The purpose of this Privacy Policy is to ensure transparency regarding the processing of personal data and to fulfill information obligations resulting from the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

1.4. Acceptance: Account Registration or ordering a Service is equivalent to full acceptance of this document and all related documents. In the event of changes to the Privacy Policy, the Client will be informed in accordance with §12.2. Lack of objection within 30 days of notification signifies acceptance of the changes. The Client has the right to terminate the agreement in the event of non-acceptance of changes.

§ 2. WHAT DATA WE COLLECT

This policy applies to data that you own (Account Data). In the case of data that you store within Digital Services (files, databases, applications), the Operator acts only as a Data Processor providing infrastructure. We do not interfere with this content, do not analyze it, and do not share it, unless upon an explicit order from a court or prosecutor's office.

2.1. Identity Data: First name, last name, age (date of birth), company name, NIP (Tax ID), residential/registered office address.

2.2. Contact Data: E-mail address, phone number (for SMS/2FA notifications).

2.3. Technical Data (Device Fingerprint): IP address, browser type (User-Agent), screen resolution, time zone, operating system - used to create a "fingerprint" of the device for the purpose of detecting multi-accounts and fraud.

2.4. Financial Data: Transaction history, payment method, transaction identifiers (Transaction ID). We do not store full payment card numbers (they are processed directly by an external Payment Operator).

2.5. Verification Data (KYC): Verification status, hash of the identity document, credibility assessment result (Scoring).

2.6. Server Logs and Security Telemetry: Login history, full activity logs in the Panel (Audit Log), as well as anonymized network traffic metadata (NetFlow/sFlow) analyzed in real-time to detect anomalies and cyberattacks.

2.7. Identity Verification (KYC) and DiDit.me:

a. Identity verification (KYC) is carried out by an external entity **DiDit.me**, which is an independent personal data controller.
b. The Operator is a separate controller regarding the processing of the verification result.
c. A detailed description of the KYC process, including the scope of data and retention periods, can be found in the Terms of Service (TOS §3.4).
d. **Legal basis:** Art. 6(1)(b) GDPR (performance of a contract).

§ 3. PURPOSES AND LEGAL BASES FOR PROCESSING

Whenever the GDPR is mentioned in the following section, it shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

3.1. Provision of Services:

a. **Basis:** Art. 6(1)(b) GDPR.
b. **Explanation:** Necessary for the performance of the contract (provision of Services, access to the Client Panel).

3.2. Payment Processing:

a. **Basis:** Art. 6(1)(b) GDPR.
b. **Explanation:** Processing vPLN top-ups and issuing invoices.

3.3. Own Marketing:

a. **Basis for data processing:** Art. 6(1)(f) GDPR (legitimate interest).

b. **Basis for electronic communication:** Art. 6(1)(a) GDPR (consent) - required in accordance with the Electronic Communications Law (PKE Art. 398, effective from 10.11.2024).

c. **Explanation:** We may process your contact data for marketing purposes (informing about news, promotions, service development). **Sending marketing e-mail or SMS messages requires your separate consent.** You may withdraw your consent at any time by clicking the "unsubscribe" link in the message or contacting support@voxihost.pl.

d. **Consent mechanism:** Consent for electronic marketing is expressed by checking an optional box during registration or at a later time in the Client Panel. The box is unchecked by default - consent is not required to create an account. Consent can be withdrawn at any time.

3.4. Tax Obligations:

a. **Basis:** Art. 6(1)(c) GDPR.

b. **Explanation:** Storing invoices for 5 years (requirement of the Accounting Act).

3.5. Security and Logs:

a. **Basis:** Art. 6(1)(f) GDPR.

b. **Explanation:** Legitimate interest: defense against DDoS, intrusions, and Abuse.

3.6. Risk Assessment (Anti-Fraud):

a. **Basis:** Art. 6(1)(f) GDPR.

b. **Explanation:** Legitimate interest: threat verification, fraud prevention.

3.7. Handling Abuse Reports:

a. **Basis:** Art. 6(1)(f) GDPR.

b. **Explanation:** Processing data of persons reporting violations (whistleblowers) for the purpose of analysis and response to incidents.

3.8. Debt Collection and Claims:

a. **Basis:** Art. 6(1)(f) GDPR.

b. **Explanation:** Debt collection, defense against chargebacks.

3.9. Voluntary Provision of Data: Providing personal data is voluntary, however, it is a necessary condition for concluding the contract. The consequence of not providing data will be the inability to create an account and use the Services.

§ 4. PROFILING AND AUTOMATED DECISION-MAKING

In the interest of infrastructure security, we use automated systems (profiling) that assess the Client's credibility.

4.1. What it consists of: The system analyzes the IP address, device fingerprint, country of origin, payment history, and verifies the presence of data in external threat databases and abuse registries (Threat Intelligence/RBL).

4.2. Effect: If the system detects a high risk (e.g., IP associated with a botnet, stolen card), registration may be automatically rejected or the service blocked.

4.3. Your Rights: You have the right to obtain human intervention. If you believe the system has made a mistake, write to us at support@voxihost.pl - an employee will verify the decision manually.

§ 5. DATA RECIPIENTS (PROCESSORS)

We transfer your data only to trusted entities that help us provide services (Processors). Instead of listing every company by name, we indicate categories of recipients (in accordance with the GDPR):

5.1. Infrastructure and Security:

a. Data Center and colocation service providers (located in the EEA).

b. Network service providers, CDN (Content Delivery Network), and protection against DDoS attacks and WAF (Web Application Firewall).

5.2. Payments: Electronic payment operators and banks (e.g., Stripe, PayPal) - to the extent necessary to process transactions.

5.3. Support and Verification: Identity Verification providers - for the purpose of preventing fraud.

5.4. Administrative Support:

a. Accounting office / Accounting system providers.

b. Law firms and debt collection companies (exclusively in the case of pursuing claims).

§ 6. TRANSFERS OUTSIDE THE EEA

We cooperate with service providers (e.g., in the field of network security or payments) who may process data in the USA. This transfer is secure and lawful based on:

6.1. Data Privacy Framework (DPF): A decision by the European Commission stating an adequate level of data protection in the USA.

6.2. Standard Contractual Clauses (SCC): Additional legal safeguards in contracts with providers.

6.3. Transferring Data to Authorities Outside the EEA: In exceptional cases, when we receive a legally binding request to disclose personal data from a public authority of a country outside the EEA (e.g., a request for legal assistance from law enforcement authorities), the transfer will occur only if the request:

a. is consistent with an international agreement (e.g., a convention on mutual legal assistance),

b. concerns a specific case and is not of a mass nature,

c. has been verified for compliance with EU law by a lawyer.

The Operator informs the UODO (Personal Data Protection Office) of every such request, unless prohibited (e.g., secrecy of the investigation).

§ 7. DATA SECURITY

We apply technical and organizational measures consistent with industry standards:

7.1. Encryption: All connections (HTTP/API) are encrypted with the TLS 1.3 protocol. Databases and disks are encrypted at rest (AES-256).

7.2. Password Hashing: User passwords are hashed with a strong algorithm (Argon2/Bcrypt) and are never stored in plain text.

7.3. Minimalization of Access: Only authorized employees have access to data (need-to-know principle), secured by two-factor authentication (2FA).

7.4. Backups: Backup copies of the Operator's administrative systems (account databases, client panel) are encrypted and stored in a separate geographical location. Note: The above does not apply to backups of data inside the Client's VPS server, for which the Client is responsible (in accordance with the Terms of Service).

7.5. Breach Procedure: In the event of detecting a personal data breach (Data Breach) that may cause a risk to the rights of users, we will report the incident to the President of the UODO within **72 hours** of its detection (in accordance with Art. 33 GDPR). In the case of high risk, we will also inform the data subjects without undue delay (in accordance with Art. 34 GDPR).

7.6. Security Tests: The Operator conducts regular security audits of the infrastructure, including penetration tests (pentests) and code reviews to identify and remove security vulnerabilities.

§ 8. RETENTION PERIOD (HOW LONG WE KEEP DATA)

8.1. Account Data: For the duration of the contract + **30 days** after its termination (buffer for errors).

8.2. Invoices: 5 years from the beginning of the year following the tax year (legal requirement - Accounting Act, Art. 74(3)).

8.3. Technical Logs: For a period of **12 months** (or another period required by applicable provisions of the Electronic Communications Law - PKE, Art. 47) for security purposes and at the request of authorized bodies.

8.4. Data Retention for Security Purposes (Prevention of Recidivism):

a. In the case of Clients blocked for a serious violation of the Terms of Service (Abuse, Fraud, Infrastructure Attacks), the Operator reserves the right to store their data (including: IP address, fingerprint, evidence of violation, correspondence) for a period of **10 years** from the date of blocking the account, based on the Legitimate Interest of the Controller (Art. 6(1)(f) GDPR).

b. The Operator may also store anonymized verification data (e.g., cryptographic hash of an identity document) for a period of up to **10 years** to prevent re-registration of persons committing serious violations.

c. The purpose is defense against claims, securing infrastructure, and securing evidence for law enforcement authorities.

d. In this regard, the right to delete data is limited. After the retention period (10 years), data is automatically deleted, unless keeping the data is necessary for defense against ongoing court or criminal proceedings.

e. **Exception for Amnesty:** In the event that a Client has successfully passed the Amnesty procedure (in accordance with the Terms of Service) and has not committed a repeated violation for a period of at least 2 years from the unblocking of the service, data from the original violation may be deleted at the Client's request. The decision is made by the Operator after verifying the absence of new incidents.

8.5. Automatic Deletion: After the retention periods specified in §8.1-8.4 have expired, data is automatically deleted from production systems and backup copies in accordance with security procedures (overwrite/shredding), preventing its recovery.

§ 9. YOUR RIGHTS AND THEIR LIMITATIONS

You have the right to:

9.1. Access Your Data: You can request a copy of the personal data we store.

9.2. Rectification of Data: You can request the correction of incorrect or incomplete data.

9.3. Erasure of Data ("Right to be Forgotten"): Provided that this right does not apply if processing is necessary for the establishment, exercise, or defense of legal claims (e.g., if you have unpaid invoices or have been banned for violating the Terms of Service).

9.4. Restriction of Processing: You can request a temporary suspension of data processing in

specific cases.

9.5. Data Portability: You can request to receive data in a structured, commonly used format (e.g., JSON).

9.6. Objection: You have the right to object to the processing of data based on a legitimate interest. The Operator may reject it if it demonstrates the existence of valid, legitimate grounds for processing that override your interests (e.g., security of the Operator's entire network).

9.7. Lodging a Complaint: You have the right to lodge a complaint with the President of the Personal Data Protection Office (UODO), ul. Stanisława Moniuszki 1A, 00-014 Warsaw.

9.8. Submitting Requests: Please direct requests regarding the exercise of the above rights to the address: support@voxihost.pl. We will respond within **1 month** of receiving the request (in accordance with Art. 12.3 GDPR). In justified cases (e.g., complexity of the request, large number of requests), we may extend this period by another 2 months, informing you of the reasons for the delay.

§ 10. PROTECTION OF CHILDREN

Our services are directed exclusively to persons who have reached the age of **16** (in accordance with the Terms of Service). We do not knowingly collect personal data from children. In the event of discovering that an account was created by a person below this age without the consent of a legal guardian, we will take steps to immediately delete such data and block the account.

§ 11. COOKIES AND LOCAL STORAGE

The website uses cookies and browser local storage (Local Storage) to a minimal extent:

11.1. Necessary (Technical): Maintaining the login session, remembering preferences (e.g., light/dark theme), preventing CSRF attacks.

11.2. Security (Cloudflare/Turnstile): Bot detection (distinguishing humans from automated systems).

11.3. No Tracking Cookies: We do not use marketing or third-party tracking cookies (e.g., Google Analytics, Facebook Pixel). We respect your privacy.

§ 12. CHANGES TO THE PRIVACY POLICY

12.1. Right to Changes: The Operator reserves the right to introduce changes to this Privacy Policy in the event of changes in legal regulations, technology, or data processing methods.

12.2. Notification of Changes: We will inform the Client of any significant change via e-mail or through a message in the Client Panel at least **30 days** in advance. Lack of objection within **30 days** of notification signifies acceptance of the changes. In the event of an objection, the Client has the right to terminate the agreement in accordance with the provisions of the TOS.

12.3. Availability: The current version of the Privacy Policy is always available on the VoxiHost.pl website in the footer of the page and in the Client Panel after logging in, in a form that allows for downloading, saving, and printing. The date of the last update is located in the header of the document.