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 " voxigames.com"

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: 14.11.2026
Last Updated: 15.10.2026

§ 1. INTRODUCTORY PROVISIONS AND DEFINITIONS

1.1. Data Controller:

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

operating the VoxiGames service (hereinafter referred to as "VoxiGames" 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 scope of the website available under the VoxiGames.com domain, the business activity of which is game server hosting. This document does not apply to other services, projects, or websites operated by the Operator under other addresses. The rules for processing End-User data on the Client's Game Servers are specified in § 12 below.

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 tantamount to full acceptance of this document and all related documents. In the event of changes to the Privacy Policy, the Client will be notified in accordance with § 13.2. Failure to object within 30 days of notification constitutes acceptance of the changes. The Client has the right to terminate the agreement in the event of non-acceptance of the 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 (game worlds, maps, plugins, databases), the Operator acts solely as a Processor providing the infrastructure. We do not interfere with such content, analyze it, or share it, unless expressly ordered by a court or prosecutor's office. A separate category consists of End-User data on the Client's Game Servers - the rules governing them are described in § 12.

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

2.2. Contact Data: E-mail address, telephone 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 device "fingerprint" 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 or authentication data for payment instruments (these are processed directly by an external Payment Operator).

2.5. Verification Data (KYC): Verification status, identity document hash, credit score result.

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, cyberattacks, and DDoS attacks against Game Servers.

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:** Article 6(1)(b) of the GDPR (performance of a contract).

§ 3. PURPOSES AND LEGAL BASES OF PROCESSING

Whenever the GDPR is referred to in the following section, it means 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:** Article 6(1)(b) of the GDPR.

b. **Explanation:** Necessary for the performance of the contract (provision of Services, access to the Client Panel and Game Panel).

3.2. Payment Processing:

a. **Basis:** Article 6(1)(b) of the GDPR.

b. **Explanation:** Processing Credits top-ups, settling the Reservation Fee and Operating Time Fees, and issuing invoices.

3.3. Proprietary Marketing:

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

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

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

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

3.4. Tax Obligations:

a. **Basis:** Article 6(1)(c) of the GDPR.

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

3.5. Security and Logs:

a. **Basis:** Article 6(1)(f) of the GDPR.

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

3.6. Risk Assessment (Anti-Fraud):

a. **Basis:** Article 6(1)(f) of the GDPR.

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

3.7. Abuse Reporting Management:

a. **Basis:** Article 6(1)(f) of the GDPR.

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

3.8. Assertion of Claims:

a. **Basis:** Article 6(1)(f) of the GDPR.

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

3.9. Voluntariness of Providing Data: Providing personal data is voluntary, yet it is a necessary condition for concluding the contract. The consequence of failing to provide data will be the inability to create an account and use the Services.

§ 4. PROFILING AND AUTOMATED DECISION-MAKING

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

4.1. What It Involves: 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 registers (Threat Intelligence/RBL).

4.2. Consequence: If the system detects high risk (e.g., an IP associated with a botnet, a stolen card), the 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@voxigames.com - an employee will manually verify the decision.

§ 5. DATA RECIPIENTS (PROCESSORS)

We share your data only with 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), DDoS protection, and WAF (Web Application Firewall) providers.

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

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

5.4. Administrative Operations:

a. Accounting office / Accounting system providers.

b. Law firms and debt collection agencies (solely in the event of asserting claims).

§ 6. TRANSFERS OUTSIDE THE EEA

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

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

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

6.3. Transfer of 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 mutual legal assistance from law enforcement authorities), the transfer will take place only if the request:

a. complies 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 shall inform the Personal Data Protection Office (UODO) of any such request, unless prohibited from doing so (e.g., by investigative secrecy).

§ 7. DATA SECURITY

We apply technical and organizational measures compliant with industry standards:

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

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

7.3. Access Minimization: Access to data is granted only to authorized employees (need-to-know basis), secured by two-factor authentication (2FA).

7.4. Backups: Backups 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 data backups inside the Client's Game Server (game worlds, maps, plugins, server databases), which are the sole responsibility of the Client (in accordance with the Terms of Service).

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

7.6. Security Testing: The Operator conducts regular infrastructure security audits, including penetration tests (pentests) and code reviews, in order to identify and eliminate security vulnerabilities.

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

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

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

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

8.4. Data Retention for Security Purposes (Protection against Recidivism):

a. In the case of Clients blocked for a serious breach of the Terms of Service (Abuse, Fraud, Attacks on the infrastructure), the Operator reserves the right to store their data (including: IP address, fingerprint, evidence of the breach, correspondence) for a period of **10 years** from the date of blocking the account, based on the Legitimate Interest of the Controller (Article 6, paragraph 1, letter f of the 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** in order to prevent re-registration of persons committing serious breaches.

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

d. To this extent, the right to erasure of data is restricted. After the retention period (10 years) has expired, data is automatically deleted, unless the retention of data is necessary for the defense against ongoing judicial or criminal proceedings.

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

8.5. Automatic Deletion: Upon the expiry of the retention periods specified in § 8.1-8.4, data is automatically deleted from production systems and backups in accordance with security procedures (overwrite/shredding), making its recovery impossible.

§ 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 stored by us.

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

9.3. Erasure of Data ("Right to be Forgotten"): Subject to the provision 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 a violation of the Terms of Service).

9.4. Restriction of Processing: You can request the temporary suspension of data processing in specific cases.

9.5. Data Portability: You can request to receive your 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 compelling legitimate grounds for the processing which override your interests (e.g., the 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: Requests regarding the exercise of the above rights should be sent to: support@voxigames.com. We will respond within **1 month** of receiving the request (in accordance with Article 12.3 of the 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. CHILD PROTECTION

Our services are directed exclusively to persons who are at least **16 years of age** (in accordance with the Terms of Service). We do not knowingly collect personal data from children. If we discover that an account has been 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. Essential (Technical): Maintaining a login session, remembering preferences (e.g., light/dark theme), preventing CSRF attacks.

11.2. Security (Cloudflare/Turnstile): Detecting bots (distinguishing humans from automated programs).

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. CLIENT GAME SERVERS - ROLE OF THE PARTIES (CONTROLLER / PROCESSOR)

This section applies to situations where the Client uses the Game Server to host gameplay for third parties (End Players). Game worlds, maps, plugins, and databases remain the property of the Client (TOS § 9.1).

12.1. Division of Roles: Regarding the personal data of End Players (including IP addresses, nicknames, game account identifiers (UUID), chat logs, character data, e-mail addresses in the case of registration on the server):

a. **The Client is the Data Controller** - the Client decides on the purposes and means of processing, establishes their own server terms of service, and fulfills information obligations towards players under Articles 13-14 of the GDPR.

b. **The Operator is solely a Data Processor** - we provide the infrastructure (computing power, disk, connection) and store data exclusively to the extent necessary to provide the Service.

12.2. No Interference: The Operator does not analyze, index, profile, or disclose the data of End Players. The exception is a legally binding request from an authorized authority, carried out in accordance with § 6.3, and actions necessary to protect the infrastructure against attacks (e.g., traffic analysis to repel DDoS).

12.3. Client's Obligations: The Client is obliged to:

a. have a legal basis for processing the data of End Players,
b. inform End Players about the processing of their data (own server privacy policy),
c. fulfill GDPR rights towards End Players and entities from whom data was acquired,
d. report a personal data breach affecting End Players to the Operator immediately after its detection - the Operator will then provide the necessary technical assistance.

12.4. Data Processing Agreement (DPA): Upon the Client's request, the Operator shall conclude a standard Data Processing Agreement (DPA) in accordance with Article 28 of the GDPR, constituting an integral part of the Terms of Service in B2B relations (TOS § 10.10).

12.5. Data Processed by the Operator as a Controller: Regardless of the above, the Operator as a Controller processes in connection with the Game Server exclusively: Client Account data (§ 2.1-2.5), security metadata and technical logs (§ 2.6), and billing data - on the terms described in § 3, § 4, and § 8.

§ 13. PRIVACY POLICY CHANGES

13.1. Right to Make Changes: The Operator reserves the right to make changes to this Privacy Policy in the event of changes in law, technology, or data processing methods.

13.2. Notification of Changes: We will inform the Client of any material change by e-mail or via a notification in the Client Panel at least **30 days** in advance. Failure to object within **30 days** of notification constitutes 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.

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