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.

DATA PROCESSING AGREEMENT (DPA)

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

This document is part of a collection of documents:

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

Effective Date: 11.12.2026

Last Updated: 11.11.2026

This Data Processing Agreement ("DPA") applies exclusively to B2B Clients when VoxiHost processes personal data on behalf of the client in connection with the provision of services. It supplements the Terms of Service and implements Article 28 of the Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR").

The DPA does not apply to Consumers; their rights and obligations regarding personal data are defined by the Privacy Policy. The B2B Client accepts the DPA by entering into a B2B Agreement or signing a separate copy. A signed copy is available upon request.

§ 1. PARTIES AND SCOPE

The processor is VoxiHost Daniel Marszałkowski, NIP 6653080651, REGON 542936383, with its registered office at ul. 3 Maja 29, 62-500 Konin ("VoxiHost", "processor").

The controller is the B2B client indicated in the account or order ("client", "controller"). A B2B Client is the entity to which a Workspace is assigned within the meaning of the Terms of Service.

This DPA covers the processing of personal data necessary for the provision of VPS hosting, related infrastructure services, DDoS protection, support, and billing. The DPA does not cover processing in

which VoxiHost acts as a separate controller (e.g., account data, KYC, payments).

The processing duration corresponds to the period of service provision, followed by the data deletion period described in section 11.

§ 2. DEFINITIONS

The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach", and "sub-processor" have the meanings given to them in the GDPR.

"Services" mean the services provided by VoxiHost under the Terms of Service, including the client panel and support.

§ 3. ROLES AND INSTRUCTIONS

The client is the controller of the personal data processed within the scope of the services. VoxiHost acts as a processor.

VoxiHost processes personal data solely on the documented instructions of the client, including those based on this DPA, the Terms of Service, the order, and settings selected in the client panel.

The client is responsible for having a legal basis for processing, providing the required information to data subjects, and ensuring that the transferred data is accurate and lawful.

VoxiHost will immediately inform the client if an instruction violates the GDPR or other applicable data protection regulations.

§ 4. PROCESSOR OBLIGATIONS

VoxiHost undertakes to:

Processing does not include the sale of personal data, its use for advertising, or disclosure to third parties, except in cases described in this DPA or required by law.

a. process personal data solely for the purposes described in this DPA and in accordance with the client's instructions;
b. ensure that persons authorized to process data are committed to confidentiality;
c. implement appropriate technical and organizational measures in accordance with Article 32 of the GDPR;
d. assist the client in fulfilling data subject requests and obligations under Articles 32-36 of the GDPR, taking into account the nature of the processing;
e. maintain a record of processing activities as referred to in Article 30(2) of the GDPR;
f. inform the client if VoxiHost believes an instruction violates applicable law;
g. make available information necessary to demonstrate compliance and allow for audits in accordance with section 12.

§ 5. CONFIDENTIALITY

Access to personal data is restricted to persons who need it for the operation, security, or support of the services. These persons are bound by confidentiality even after the termination of cooperation.

VoxiHost does not access client content unless necessary to resolve a ticket authorized by the client, prevent abuse or security incidents, or as required by law. Regarding abuse prevention and security, VoxiHost may act as a separate controller based on Article 6(1)(f) of the GDPR; it shall inform the Client of this.

§ 6. SECURITY MEASURES

VoxiHost implements the technical and organizational measures described in Annex II, including access control, network protection, virtual instance isolation, backups, event logging, and incident response.

The client is responsible for their own configuration, access credentials, access management, application security, and all content and end-user data stored in the services.

VoxiHost may update the measures, provided that the overall level of protection is not lowered.

§ 7. SUB-PROCESSORS

The client grants general authorization to VoxiHost to use sub-processors for the processing described in this DPA. The current list is available in Annex III.

VoxiHost will notify the client at least 30 days in advance of adding or changing a sub-processor processing personal data. The client may raise a reasoned objection regarding data protection. If the objection cannot be resolved, the client may terminate the affected services.

VoxiHost imposes data protection obligations on sub-processors that are no less protective than those resulting from this DPA and remains responsible for their performance.

§ 8. DATA SUBJECT RIGHTS

Taking into account the nature of the processing, VoxiHost assists the client in fulfilling requests from data subjects regarding their rights under the GDPR.

The client is responsible for responding to data subject requests. If VoxiHost receives a request directly, it will forward it to the client immediately, unless the client has authorized VoxiHost to respond.

VoxiHost may provide self-service tools in the client panel for exporting or deleting account data.

§ 9. DATA TRANSFER OUTSIDE THE EEA

Main processing takes place within the European Economic Area. Some sub-processors (e.g., Cloudflare) and separate controllers (e.g., payment providers) may process limited data outside the EEA.

In the case of transferring personal data outside the EEA, VoxiHost ensures the application of an adequacy decision or appropriate safeguards, such as the European Commission's standard contractual clauses.

§ 10. PERSONAL DATA BREACH

VoxiHost will notify the client immediately, and in any case within 48 hours of becoming aware of a personal data breach concerning client data, providing available information and updating it as circumstances are determined. This provision does not relieve the client of obligations under Articles 33 and 34 of the GDPR; VoxiHost will provide the client with reasonable assistance in reporting.

The notification will describe, to the extent known, the nature of the breach, categories and approximate number of data, probable consequences, and measures taken or planned. The notification contains contact details of the person responsible for the report (support@voxihost.pl).

VoxiHost will cooperate in the client's investigation and any potential reports to supervisory authorities or data subjects. The notification does not constitute an admission of guilt or liability.

§ 11. DELETION AND RETURN OF DATA

Upon termination of services, the Client chooses to return or delete the data. If the Client does not specify, VoxiHost will delete the data within 30 days, unless a longer retention period is required by law. The return takes place in a structured format within 30 days.

Remaining copies in backups will be deleted within 90 days as part of the normal rotation cycle.

The Client may export their data during the term of the agreement using tools available in the client panel. VoxiHost will provide reasonable assistance with export requests submitted before the end of services. Upon the Client's request, VoxiHost will return the data in a structured format before deletion.

§ 12. AUDITS AND COMPLIANCE

VoxiHost will make available to the client the information necessary to demonstrate compliance with this DPA, including the documents referred to in the DPA.

The client may conduct an audit once a year or more frequently if required by a supervisory authority, upon at least 30 days' written notice. Audits are by default conducted remotely and must not compromise the security or confidentiality of other clients.

Audit costs are borne by the client. VoxiHost may require the signing of a non-disclosure agreement before providing audit materials.

§ 13. LIABILITY

Liability arising from this DPA is subject to the limitations and exclusions set forth in the Terms of Service, provided that no provision of this DPA limits liability that cannot be limited under applicable law. In particular, nothing in this DPA limits VoxiHost's liability towards data subjects under Article 82 of the GDPR or administrative fines under Article 83 of the GDPR; any limitation applies solely to the relationship between the client and VoxiHost to the extent permitted by law.

§ 14. TERM AND AMENDMENTS

This DPA enters into force upon its acceptance by the client or upon the commencement of the use of services and remains in effect for the entire period during which VoxiHost processes personal data on behalf of the client.

VoxiHost may propose amendments to the DPA. Amendments require the client's written acceptance; until such acceptance, the previous version remains in effect. Amendments required by law enter into force by operation of law.

§ 15. GOVERNING LAW

This DPA is governed by Polish law. Disputes are subject to the jurisdiction of the courts competent for the processor's registered office, unless mandatory provisions of law provide otherwise.

Annex I - Processing Details

This Annex describes the processing carried out by VoxiHost on behalf of the client.

a. Data subjects - end users of the client's services and visitors whose data is processed within the scope of the services.
b. Categories of personal data - technical logs, IP addresses, communication with support, and content and data of end users stored by the client in the services. Account, KYC, and billing data are processed by the Operator as a separate controller and are not covered by this DPA.

c. Special categories of data - The services are not intended for the processing of special categories of personal data. The client may not transfer such data unless they have a legal basis and appropriate safeguards.

d. Purpose - Provision and maintenance of services, support, billing, security, abuse prevention, and legal compliance.

e. Duration - The period of service provision, followed by the deletion periods described in section 11.

f. Frequency - Continuous for the duration of the service provision.

Annex II - Technical and Organizational Measures

a. **Access control:** individual accounts, access based on the principle of least privilege, and authentication of administrative systems.

b. **Network protection:** firewalls, DDoS filtering, and monitoring of the VoxiHost network.

c. **Isolation:** virtual instances are separated from each other and from management systems.

d. **Encryption:** TLS 1.2/1.3 for data transmitted between clients and services; encryption at rest (AES-256) for systems managed by VoxiHost (account databases, client panel, infrastructure backups). Data within the client's VPS instance is not encrypted by VoxiHost unless the client enables encryption on their own.

e. **Backups:** daily disaster recovery backups of the infrastructure and optional client snapshots.

f. **Logging and monitoring:** security-relevant events are logged and analyzed for investigation and incident response purposes.

g. **Vulnerability management:** software and infrastructure are updated and checked for security issues.

h. **Incident response:** documented process for handling security incidents and personal data breaches.

i. **Confidentiality:** persons having access to client data are bound by confidentiality.

j. **Data minimization:** only data necessary for the provision and security of services is collected.

Annex III - Sub-processors and Separate Controllers

SUB-PROCESSORS (process client data on behalf of VoxiHost):

a. Cloudflare, Inc. - Turnstile, bot protection and CDN. - USA (DPF or SCC); processor for bot detection, separate controller for its own purposes.

b. Rotorfly Europa GmbH & Co. KG (iNTERWERK) - server colocation and Data Center infrastructure in Frankfurt am Main. - EEA (Germany); registered office: Pezolddamm 156, 22159 Hamburg, HRA 99509, Amtsgericht Hamburg.

SEPARATE CONTROLLERS / OPERATOR'S OWN DATA PROCESSORS:

a. didit.me - Identity verification (KYC) - Operator's own data; verification processor commissioned by VoxiHost, separate controller for its own purposes. Does not process client data within the meaning of DPA §1.

b. Stripe Payments Europe, Ltd. - Payment processing for cards, wallets, and Link. - Ireland / EEA and United States (DPF or SCC).

c. PayPal (Europe) S.à r.l. et Cie, S.C.A. - PayPal payment processing. - Luxembourg / EEA.

d. NOWPayments (FD Transfers LLC) - Cryptocurrency payment processing. - Saint Vincent and the Grenadines; SCC + TIA.

e. Accounting office / accounting system provider - accounting services. - EEA.

f. Law firm / debt collection agency - claim enforcement. - EEA (only if necessary).