

Privacy Policy

Last updated: 9 September 2026

How information is handled when you use GridHunter.

1. About this policy

GridHunter is an independent Founding Beta project operated by a private individual. The operator determines how personal data are used for the service. Contact for privacy questions and requests: support.gridhunter@gmail.com.

This policy covers the website, User Portal, VPN service and official applications. It also covers support communications and payment information received by GridHunter. Payment providers and other independent third parties explain their own processing in their privacy notices.

2. Account and sign-in information

We process your nickname or account display name, email address, account identifiers, account status and registration and sign-in dates. You do not need to provide your legal name. If you have supplied an optional Telegram identifier through an account feature, that information may also be associated with your account.

Account passwords are stored as password hashes. Sign-in sessions use a browser cookie and a server-side token hash. Session records also include an IP address, browser or application information and activity timestamps. Password recovery uses a time-limited link; a token hash is stored by GridHunter and the link itself is sent by email.

3. Devices, access and usage

When an official application requests its connection settings, we may process an installation identifier or its hash, device name, model, platform, operating-system version, application version, IP address and last activity time. A device name supplied by an application may reflect a name configured on the device.

Installation identifiers help recognise an application installation and apply device limits. Hashing an identifier does not make it anonymous where it remains linked to an account.

We process access status, assigned plans or beta access rules, expiry dates, traffic allowances, device limits and connection credentials. Usage records may include uploaded and downloaded data volumes, activity times and the server or access configuration used.

4. Technical records and network information

Website, application and server records may contain IP addresses, request times, browser or application details, requested service URLs, errors and security events. Account events may also contain account details or a hashed email address.

VPN operation involves processing connection information, including destination addresses and DNS requests where applicable. Technical or diagnostic logs may retain destination IP addresses or domain names. GridHunter does not offer a guarantee that connection metadata are never logged, or that using the service makes you anonymous.

5. Support and payment information

If you contact us, we process your contact details, correspondence and attachments. Please include only what is needed for your request and avoid sending passwords, complete connection credentials or unrelated personal information.

Where a payment option is used, we may process account and transaction identifiers, amount, currency, payment status, timestamps and information about refunds, disputes or renewals. A payment provider may also make buyer contact details available where needed to resolve a payment or cancellation request.

Payment-card details are entered with the payment provider; GridHunter does not ask you to send full card numbers or card security codes. Service emails, including recovery links, pass through email providers.

6. Purposes and legal grounds

We use account, session, device and access information to provide the service you request, authenticate you, deliver connection settings, apply access limits and assist with account recovery. Where applicable, this processing is necessary to perform our agreement with you or take steps at your request.

Security records and necessary diagnostics support our legitimate interests in preventing abuse, protecting accounts and infrastructure, investigating failures and maintaining a reliable service. These interests must be balanced against your rights. Support and transaction records help us handle your requests, resolve disputes and meet applicable legal obligations.

If an optional activity requires consent, we will seek that consent separately. You may withdraw it without affecting processing already carried out lawfully. Accepting the Terms does not give blanket consent to unrelated uses of your data.

We do not sell personal data or use VPN activity to build advertising profiles. Information necessary for authentication or delivery of the service cannot be omitted while still using the affected feature. You can choose not to make a support payment or send optional diagnostic information.

7. Service providers and other recipients

Information may be handled by providers supporting hosting, VPN infrastructure, content delivery, DNS, email and payment processing. The recipients depend on the feature and connection route you use.

Relevant services may include Hetzner, OVH and RUVDS for server infrastructure; Selectel for content delivery; Resend for service email; Google Gmail for support correspondence; and Lava.Top for payments. Cloudflare and network relay services may also be involved where used for the relevant connection or infrastructure function.

Providers receive information needed for their part of the service. Payment providers may process additional information under their own legal obligations. Information may also be disclosed where legally required, to respond to a valid legal request, or where necessary and lawful to protect rights and address abuse. We do not promise disclosure of data we do not hold.

8. International processing

Service infrastructure and providers operate in more than one country. Depending on the service used, data may be processed in Finland, Poland, Russia, Serbia and other countries where providers operate. Choosing a VPN exit location does not determine where all account, email or payment records are stored.

Cross-border processing remains subject to applicable data-protection requirements. Where a transfer requires a recognised safeguard or another lawful transfer mechanism, it must be covered by that mechanism. Contact us for information about recipients, processing locations and safeguards relevant to your data.

9. Cookies and local information

The User Portal uses a session cookie to keep you signed in. A normal session is valid for up to 30 days unless ended or revoked earlier. Blocking this cookie may prevent sign-in from working. Applications also keep connection settings and installation information needed to operate.

A password reset link is valid for 30 minutes and can be used once. Expiry of a cookie or reset link ends its use for authentication; it does not by itself erase every associated server record or email copy. Third-party checkout pages may use their own cookies as described by the provider.

10. Retention and account deletion

Account and access records are kept while needed to maintain your account and administer the service. Technical, security and usage records are retained according to their purpose, the need to investigate incidents and the retention settings of the relevant system. There is no single retention period covering all systems and providers.

Support correspondence is retained while needed to resolve the request and related disputes. Transaction information may need to remain after account closure for legal, accounting, fraud-prevention or dispute-resolution purposes. The relevant obligation or unresolved matter determines whether continued retention is necessary.

Account closure does not automatically erase all account, event or backup records. To request erasure, contact us. We will assess the request and explain any information that must be retained and why. Backup and provider copies may remain until their applicable retention cycle ends; erasure must also be considered when restoring a backup.

11. Your choices, rights and security

Subject to applicable law, you may request access, correction, erasure, restriction, portability or object to processing. You may also withdraw consent where processing relies on it. We may ask for proportionate information to verify your request. We will respond within the applicable legal time limit and explain any lawful extension or refusal.

Access and device limits may be applied automatically. If you believe a restriction is incorrect, contact support for review. You may complain to the competent data-protection authority. In Serbia, this is the Commissioner for Information of Public Importance and Personal Data Protection: poverenik.rs.

We use measures such as password hashing and access controls, but no internet service can guarantee absolute security. GridHunter is intended for adults aged 18 or over. Contact us if you believe a child has provided personal data. Material changes to this policy will be communicated where required, and its updated date will identify the current text.

For questions or requests, email support.gridhunter@gmail.com.