Rules and acceptable use

YRNA VPN Terms of Use

These Terms govern the use of YRNA VPN and apply to every user who launches the bot, confirms the documents, activates a trial, imports a subscription, pays for access, or contacts support regarding the service.

1. Operator identification

Operator name: YRNA VPN service operator.

Important: if exact legal details, registration data, or the service address differ from the values below, they must be updated before final legal approval of these documents.

Support email: support@yrnavpn.com.

Telegram support: @yrna_support (https://t.me/yrna_support).

Support intake hours: Электронные обращения принимаются круглосуточно; ответы предоставляются в разумный срок в порядке очереди.

2. Acceptance of the Terms

Confirmation of the Terms in the Telegram bot, activation of a trial, import of the subscription, use of a connect link, or payment for a plan may each constitute acceptance of these Terms in the applicable part.

If the user does not agree with the Terms in whole or in part, the service must not be used.

The Russian-language version is the primary version for Russian-language public communication. The English version is an informational translation unless the operator expressly states otherwise.

3. Scope of the service

The service provides digital access to VPN infrastructure, routes, subscription links, connection helper pages, and related support and account-management surfaces that the operator treats as part of the product.

The operator may change protocols, addresses, internal topology, route delivery, or connection flow where required for security, reliability, or anti-abuse reasons.

4. Personal access and transfer restrictions

Access is intended for personal use unless a selected plan explicitly allows another model.

The user may not resell access, publish credentials, share connect links for collective use, or otherwise use the service as resale infrastructure without express written consent from the operator.

5. Prohibited use

The service may not be used for spam, malware, phishing, credential attacks, carding, DDoS, abuse

against third-party systems, sanctions evasion where prohibited by law, or any other unlawful activity.

The service may not be used in a way that creates disproportionate load, harms node stability, or intentionally hides traces of unlawful conduct.

Attempts to gain administrative access, internal tokens, hidden runtime endpoints, or other non-public service internals are prohibited.

6. Devices, limits, and technical controls

Device limits are defined by the selected plan and may be enforced through inventory controls, runtime hardware limits, fingerprints, import history, and anti-abuse signals where technically available.

The operator may temporarily restrict or revoke a device where signals indicate abuse, inventory mismatch, compromise risk, or other security issues.

Failure to import a subscription on a particular client or device may stem from the service, client software, ISP conditions, or the user's local environment.

7. Availability, maintenance, and route changes

The service is provided on an as-available basis. The operator does not promise uninterrupted availability, identical route quality, or permanence of any specific location.

The operator may conduct maintenance, disable or hide nodes, change runtime profiles, or replace routes without separate user approval.

Partial route unavailability, ISP filtering, DPI blocking, or third-party platform restrictions do not by themselves mean the operator breached its obligations if the service is otherwise reasonably provided.

8. Payments, renewals, and refunds

Price, currency, discount, promo logic, term, and enabled payment methods are shown before order confirmation and form part of the specific transaction.

If the service ever offers recurring charges or auto-renewal, that scenario must be separately and clearly accepted by the user before the first recurring charge.

After the user withdraws consent to recurring charges, auto-renewal, or the use of previously saved payment data, the operator must not initiate new recurring charges based on the previously saved data without a fresh separate consent.

Once payment is confirmed, the operator grants or extends digital access according to the paid order. The exact delivery moment depends on technical execution.

Refunds for digital services are reviewed individually in cases such as duplicate charge, non-delivery, or a material technical inability to provide the paid access.

9. Suspension and termination

The operator may restrict, suspend, or terminate access in case of Terms violations, payment abuse, chargeback, fraud risk, security risk, infrastructure protection needs, or applicable legal / provider obligations.

The user may stop using the service at any time, but that does not automatically create a refund right for digital access already started unless required by mandatory law or granted by the operator in a specific case.

10. Liability

The operator is not liable for indirect losses, lost profit, third-party blocking, app-store restrictions, ISP filtering, sanctions, force majeure, or other matters outside reasonable control unless mandatory law provides otherwise.

Nothing in these Terms excludes mandatory consumer rights that cannot lawfully be waived.

11. Changes

These Terms are effective from April 7, 2026.

The operator may update this document. The current published version applies to new user actions from its effective date unless mandatory law requires another approach.