

YRNA VPN Privacy Policy

This Policy explains which personal and technical data the YRNA VPN operator may process, why the data is processed, how it may be shared, how long it may be stored, and how a user can submit a privacy-related request.

1. Operator and privacy contact

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) (https://t.me/yrna_support).

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

Privacy / legal contact: .

2. Data categories

The operator may process Telegram identifiers, usernames, language preferences, bot interaction metadata, onboarding status flags, contact email, referral metadata, wallet / promo / discount data, subscription status and term, payment events, and support history.

The operator may also process device inventory, device titles, fingerprints, runtime-confirmed identifiers, hardware identifiers, import history, connect history, audit logs, and other technical metadata generated during normal service operation.

When the user contacts support, additional materials such as issue descriptions, attached files, logs, IP addresses, and communications may be processed where reasonably necessary to resolve the case.

3. Processing principles

The operator proceeds on the basis of lawfulness, purpose limitation, data minimization, accuracy where relevant, and retention no longer than reasonably necessary for the declared purposes.

Where a data category is no longer needed for service delivery, infrastructure protection, dispute handling, or another valid legal basis, the operator should stop using it or move it into a legally permissible retention state.

4. Purposes of processing

Data is processed to identify the user, provide trial and paid access, enforce device limits, prevent abuse, support payments, answer support requests, maintain auditability, and protect the service

infrastructure.

Some technical data is processed to detect anomalies, revoked devices, compromised signals, broken imports, chargeback-related risk, and other situations in which the operator must verify whether a service was or was not properly delivered.

5. Legal bases

The operator proceeds on the basis that processing is necessary to provide the requested digital service, perform the user's order, maintain security, prevent abuse, and comply with applicable legal obligations.

Where the interface requires document confirmation, the user also gives consent to the processing reasonably necessary for service delivery and support/payment workflows.

6. Sharing with third parties

Data may be shared with technology and contractual partners required for delivery, including Telegram, runtime vendors, payment providers, hosting providers, monitoring and backup systems, logging systems, and anti-abuse infrastructure.

The scope of sharing is limited to what is needed to provide the service, process the payment, resolve an incident, comply with law, or protect the operator and users.

User data is not sold as a standalone commercial dataset.

7. Cross-border and distributed infrastructure processing

Because the service infrastructure and vendors may be located in multiple jurisdictions, certain technical and service data may be processed outside the user's country where this is necessary for service delivery.

Where applicable law requires advance notice to a supervisory authority, local collection of personal data, or compliance with special cross-border transfer conditions, the operator proceeds on the basis that such requirements must be respected in the applicable part.

Where applicable law imposes specific conditions or restrictions on cross-border transfers, the operator proceeds on the basis that such conditions must be respected in the applicable part.

8. Retention

Payment, support, audit, security, and anti-abuse records may be stored for as long as reasonably necessary for service delivery, access restoration, dispute handling, accounting, incident investigation, and the protection of the operator's rights.

Some technical identifiers may be retained beyond the active subscription term where needed for fraud prevention, replay protection, device revocation, dispute evidence, or operational history restoration.

9. User rights

Subject to applicable law, the user may request access to their data, correction of obvious inaccuracies, deletion of data no longer necessary for the stated purposes, or clarification of the categories and purposes of processing.

The user may also withdraw consent in the part of processing that relies specifically on consent rather than another independent legal basis; such withdrawal does not invalidate prior lawful processing and may affect the operator's ability to continue providing the service.

If the user believes their rights have been violated, the user may use the administrative or judicial remedies available under applicable law.

Requests should be sent to . The operator may request reasonable identity confirmation and proof that the request is connected to the relevant account.

10. Security

The operator uses access tokens, role separation, audit logging, rate limiting, private admin access, backups, and other technical and organizational measures appropriate to the current service architecture.

No online service can guarantee absolute security; the user should also protect their Telegram account, devices, email, and payment instruments.

11. Publication and updates

This Policy is published in open access on the public service domain as a PDF document. The Russian-language version remains the primary version for Russian-language public communication unless mandatory law requires otherwise.

This Policy is effective from April 7, 2026.

The current published version applies from the effective date of the updated version unless mandatory law requires another approach.