SpinWizRoulette Privacy Policy

Revised 12 November 2026. Effective date: 14 November 2026.

This notice covers SpinWizRoulette, our website, subscriptions and support.

1 Who is responsible

The individual trading as SpinWizLab in Sweden, described in section 1 of the accompanying Terms of Service, is the controller of the personal data we process for this service.

- Email: info@spinwizlab.com.
- Location: Stockholm, Sweden.
- Website: https://www.spinwizlab.com.

2 Information we receive and why

- **Accounts and access:** account identifiers, email, sign-in information and license/access status, supplied by you and our authentication provider, Clerk. We use these to provide your account and requested access, on the basis of our contract with you or steps you request before purchase.
- **Purchases:** Whop and its payment providers process monthly checkout and billing. Where offered, NOWPayments processes separate crypto purchases. We receive account and order, invoice, payment or membership references, amounts, currency, payment status, access dates and cancellation/refund records needed to administer access and billing. Crypto payment providers and public blockchains also process transaction and wallet information; blockchain records can be public and may not be erasable by us. Contract performance is the basis for supplying your purchase; accounting and tax duties are the basis for required transaction records. Do not send full card details, wallet private keys or recovery phrases to the app or support.
- **Optional cosmetic unlocks:** we use linked account identifiers and relevant action or membership verification records to check requested eligibility and prevent false or duplicate claims. Our processing purpose and intended legal basis are our legitimate interests in administering voluntary cosmetic benefits fairly and protecting the verification process. Some community services also send us action records, including account identifiers and event times, before an account is linked; the current implementation stores these records and can match them when you later connect your account. This pre-link processing is separate from a customer's request and requires its own necessity, balancing, transparency and retention safeguards. Following a community account is not treated as consent to all our processing. You can object or request deletion by contacting info@spinwizlab.com; we assess the request and any lawful reason for limited continued retention. Cosmetic verification is separate from paid product access.
- **Requested launch email:** if you ask to be told when new purchases open, we store your email, request time, the permission you gave and a removal reference, to send the requested one-time notice on the basis of consent. This is separate from an ongoing marketing subscription. You can withdraw the request through its removal link where supplied, or by emailing info@spinwizlab.com.
- **Support:** we receive your contact details, messages, bug reports and attachments you choose to send. We use them to investigate and answer your request, on the basis of contract

performance where needed to supply the service, or our legitimate interest in answering other enquiries.

- **Connection and security records:** our services receive IP addresses, request times, headers and service responses. We use necessary records to operate and secure the service, prevent abuse and resolve incidents, based on our legitimate interests in reliable and secure operation. Necessary service connections also support performance of our contract.

We may use relevant records to establish or defend legal claims, based on our legitimate interest in handling disputes, or to meet a binding legal obligation. We balance legitimate interests against your rights. Optional diagnostic sharing has a separate consent basis, described below.

Without necessary account, payment or license information, we may be unable to supply the relevant function. Optional diagnostics are not a condition of purchase or continued paid access. We do not sell customer personal information or use private strategies or diagnostic content for advertising.

3 License checks and local app data

The app sends your license key and a random computer activation credential securely to our service to check entitlement, restrictions, expiry and the one-computer activation limit. The credential is encrypted locally for the current Windows user and persists after logout. The server stores an account-specific digest and activation/validation times, rather than the raw credential. This check does not collect hardware serial numbers or a computer name. We use it to supply and protect the licensed access under our contract, with necessary anti-abuse records also supporting our legitimate interest in preventing license misuse.

The response includes account email, access level, expiry and unlocked theme names. Checks occur at activation, startup and periodically during use. They automatically allow or block access; an unsuccessful check can lock the workspace and stop active functions. Contact info@spinwizlab.com for human review of an incorrect access decision or to request an activation transfer. Deleting a local credential does not delete the server activation record.

Settings, strategies, calibration profiles, personal spin-history caches, betting audit records and recovery logs are stored locally on your computer. Local recovery logging can continue when optional sharing is off. These files are not automatically uploaded as part of diagnostic sharing. Local copies and backups remain under your control.

Guided and Automatic Betting use relevant mouse/window information and local screen regions while enabled. Screen processing stays on your device; these functions do not upload a desktop recording or read casino login credentials, browser cookies or session tokens. Information you separately choose to attach to support is handled as support content.

4 Optional diagnostics and bug reports

Diagnostic sharing is controlled in the app's privacy settings under Help. Capture and transmission begin only after the current notice is confirmed with sharing enabled. You can disable sharing there without losing paid access. Necessary licensing and security connections are separate.

Shared diagnostics can include app/version and operating-environment information, error types and limited error traces, event times, predefined app actions, feed status, uptime, and random installation/event identifiers. These records help investigate faults and reliability. Reports can be associated with your licensed account; random identifiers do not make them anonymous.

Automatic diagnostic payloads exclude license keys, authentication tokens, email addresses, full local file paths, screenshots, typed text, strategy/calibration contents, personal spin databases and casino/browser traffic. Servers still receive normal connection metadata, including IP addresses.

In-app bug reports require sharing to be enabled and a separate submission of your reviewed summary and optional details. Opening the form sends nothing. Do not include secrets or unrelated personal information. You can use email support without enabling diagnostic sharing. Saving a support file creates a local file; it is sent only if you choose to share it.

Turning sharing off stops future optional capture and sending and clears pending local reports from the delivery queue. It does not automatically delete reports already received or all local diagnostic history. Email us to request deletion of server-held data. Withdrawing consent does not affect the lawfulness of earlier processing.

5 Live sources, providers and recipients

The current desktop obtains live and archived results through the authenticated SpinWiz results service. We receive ordinary connection metadata, the requested table and short-lived access authorization. Collection from upstream results sources runs on our systems; this desktop does not connect directly to those sources or forward your casino credentials to them. Older app versions may have used direct connections. Central table results are not a copy of your private strategies or personal betting history. Version checks and downloads also contact our services and generate normal connection records.

The seller and providers receive information needed for their role:

- **Clerk:** accounts and authentication.
- **Whop and its payment providers:** monthly checkout, membership and billing.
- **NOWPayments:** separate crypto checkout, payment confirmation and related payment handling, where offered.
- **Community platforms:** linked-account information and action or membership verification for optional cosmetic unlocks, including the action records described in section 2.
- **Vercel:** website and API hosting, download and requested-launch-email storage, and website analytics.
- **Supabase:** server-side records and history storage.
- **Sentry:** optional error reporting when enabled.
- **Zoho Mail:** email correspondence and support.

Providers processing data on our instructions do so under appropriate arrangements. Providers acting independently, including for payment compliance or their own account services, apply their own privacy notices. Social connections and external links also involve the selected service's own processing. We may share necessary information with advisers or authorities where legally required or needed to establish or defend a claim.

6 International processing

We operate from Sweden. Our providers operate internationally, so information may be processed in the EU/EEA, the United States and other countries used by the relevant service, its subprocessors or support teams. The location depends on the service and selected hosting region. Regional database hosting does not necessarily exclude support or other processing from elsewhere.

The providers' published arrangements describe US and international operations for Clerk, Vercel, Whop and Sentry; Supabase also describes Singapore and US support arrangements, and Zoho describes international support, including India. Community platforms operate internationally under their own notices. NOWPayments' operator is incorporated in Saint Vincent and the Grenadines; incorporation alone does not identify every processing location or transfer safeguard.

For transfers outside the EU/EEA, the applicable protection must be an EU adequacy decision, including eligible transfers to currently certified US organisations, or appropriate safeguards such as approved standard contractual clauses and supplementary measures where required. The mechanism depends on the recipient and transfer. Independent providers explain their own arrangements in their notices. Contact info@spinwizlab.com for the countries, recipients and safeguards relevant to your data, or to request a copy of applicable safeguards.

7 Retention

We delete or irreversibly anonymize data when its retention period ends, except where limited preservation is required for a legal duty, specific security investigation or dispute.

- **Accounts and licenses:** while needed to maintain the account and licensed access. After a verified closure or erasure request, we assess removal of account and activation records and retain only the parts still needed for an outstanding purchase, refund, dispute, specific security investigation or legal duty. Requests are handled manually; deleting a sign-in account does not automatically erase every associated licensing, payment or verification record. We explain any justified retention or permitted extension when answering your request.
- **Accounting records:** for the legally required period. Where Swedish bookkeeping requirements apply, generally seven years after the end of the calendar year in which the relevant financial year ended.
- **Optional unlock records:** linked identifiers and relevant evidence are retained while needed to administer eligibility, honour an earned benefit or investigate a specific false or duplicate claim. Matched and unmatched action records currently have no fixed automatic expiry. Their continued retention is subject to the stated purpose, data-minimisation duties and applicable erasure and objection rights; a possible future claim is not an unlimited-retention entitlement. Temporary connection authorisations are valid for ten minutes; expiry prevents use, while physical cleanup occurs during subsequent connection attempts. Unlinking a provider does not itself erase stored evidence; contact us for review and deletion.
- **Launch-email requests:** until the requested one-time launch notice has been sent, you withdraw the request, or the planned notification is abandoned. The pending address and no-longer-needed request record are then removed through the removal function or manual administration, apart from limited evidence needed to record permission or withdrawal, prevent an unwanted repeat message or resolve a dispute. A delayed launch does not automatically expire the request; you may withdraw at any time through the supplied removal link or by contacting us.
- **Website analytics:** provider-held event data follows the analytics service's applicable retention settings. We use statistical reports while relevant to understanding and improving website use, subject to minimisation and retention requirements. Reporting availability and physical retention are different. Cookie settings controls future collection, not the retention of data already received; contact us for a privacy request.
- **Support:** while the enquiry is active, and afterwards only while the correspondence is needed for follow-up, a warranty or other claim, a dispute, security investigation or applicable recordkeeping duty. The purpose and applicable claim period determine continued retention;

unrelated attachments and unnecessary personal details should not be kept merely because the email thread remains useful. Support erasure requests are assessed manually.

- **Server diagnostics and bug reports:** while needed to investigate the reported fault, maintain service reliability or resolve the associated case. Closed-case history is retained only for relevant follow-up, recurring-fault investigation, security or legal claims. Operational records follow their configured cleanup rules, while unresolved reports require case review. Copies held by Sentry or another reporting provider follow the applicable project retention settings and privacy arrangements. You may ask us which records and period apply to your report.
- **Backups:** deletion from active systems can precede expiry of a backup copy under the relevant provider's backup cycle. Backup copies are kept for recovery, access is restricted, and an applicable deletion must be reapplied if a backup is restored. The cycle depends on the service and selected configuration; we do not promise immediate removal from every backup or from public blockchain records.
- **Local files:** diagnostics use limited storage and rotation; saved strategies, histories, exports and your backups remain until deleted or overwritten on your device.

8 Website analytics and cookies

Optional Vercel Web Analytics stays off until you accept it in the website's cookie preferences. It helps us understand visits and improve the site, processing page-view information such as page path, referrer, approximate location and browser/device category. Our filter removes page URL query strings and fragments, excludes administrator/API routes and certain sensitive referrers, and replaces community post identifiers with a general path. Normal network metadata is still received by the service when analytics is enabled. This choice is separate from the desktop diagnostics control.

The basis for optional website analytics is your consent. Accept optional and Reject optional are equally available; leaving the choice unanswered keeps analytics off. Open Cookie settings using the persistent button or footer link to change and save your choice, or visit https://www.spinwizlab.com/cookies for information. Rejection does not remove sign-in, browsing or paid access. Withdrawing permission stops future analytics and reloads the page to unload the analytics script. It does not affect the lawfulness of earlier processing or automatically erase data already received. Contact info@spinwizlab.com for a privacy request.

The website also uses storage needed for sign-in, session security and requested preferences. Blocking it can prevent those functions. Checkout, social platforms and other external services apply their own controls. Any non-essential storage or tracking requiring consent must stay off until permission is given; refusal must not remove paid access.

The privacy choice is stored in `spinwiz-cookie-preferences`, with its version and time, for 180 days of validity. Expired local entries may remain until replaced or cleared. If saving a rejection fails, the necessary first-party `spinwiz-analytics-denied` cookie can remember it for 180 days. Neither contains a tracking identifier. If both storage methods fail, the choice applies to the current visit.

The storage used for requested website functions includes:

Provider or function	Purpose and examples	Duration and available control
SpinWizLab appearance preferences	Browser local storage named `spinwiz-theme` and `spinwiz-theme-archived` stores the selected or previous appearance.	No fixed expiry; values remain until replaced or cleared through your browser's site-data controls.
Clerk authentication	Sign-in, session continuity and security cookies, including a session cookie such as `__session` where issued.	Cookie expiry attributes and configured session settings apply, rather than a token's lifetime. Signing out invalidates the session; clearing cookies can sign you out.
Whop, NOWPayments and linked community services	Storage used by the selected external checkout, sign-in or connection service under its own notice.	Provider expiry attributes and controls apply. Review its notice and browser site data; some cookies are on the provider's origin.

Vercel describes request-based visitor identification without third-party cookies and a visitor hash that is discarded after 24 hours. This is separate from the retention of event statistics and ordinary hosting or security logs. Our optional analytics waits for your choice regardless of this cookie-free design. See Vercel's analytics privacy explanation and Clerk's session information. Your browser's site-data viewer shows the cookies, storage entries and expiry attributes actually present for your current visit.

9 Your rights and contact

Depending on applicable law and the processing basis, you can request access, correction, erasure, restriction and data portability. You can object to processing based on legitimate interests and to direct marketing, and withdraw consent at any time.

Contact **info@spinwizlab.com** to exercise these rights. We may need proportionate identity verification. Requests are normally free and answered within one month, subject to legally permitted exceptions or extensions. Erasure may be limited by necessary legal retention. Deleting local files does not cancel subscription billing; you can ask us to coordinate account deletion and cancellation.

You also have the right to complain to a competent data protection authority, particularly in the EU/EEA country where you live or work, or where the alleged infringement occurred.

10 Security, age and changes

We use appropriate security measures, including encrypted transport and access controls. The product is for adults aged 18 or over, or the higher applicable legal age. Contact us if a child has supplied personal information.

We update this notice when data practices change and provide any legally required notice or consent choice. Updating the notice alone does not give consent to a new optional purpose.