StriveSumma Privacy Policy

Effective Date: March 23, 2026

Last Updated: March 23, 2026

Sheepdog Design Studio LLC ("StriveSumma", "we", "us", or "our") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use the StriveSumma platform, including our website, mobile applications, and related services (collectively, the "Service").

By accessing or using the Service, you agree to this Privacy Policy. If you do not agree with the terms of this Privacy Policy, please do not access or use the Service.

1. Information We Collect

1.1 Information You Provide Directly

Account Information: When you register for an account, we collect:

- Email address (used as username)
- Password (encrypted and never stored in plain text)
- Name
- User role (Athlete, Coach, or Administrator)
- Date of birth (for age verification)

Profile Information: Depending on your role and subscription, you may provide:

- Genetic markers (ACTN3 genotype: RR/RX/XX; FTO genotype: TT/AT/AA)
- Physical limitations (arthritic joints, running restrictions, jumping restrictions, plyometric restrictions, custom limitations)
- One-rep maximum (1RM) baselines for key lifts (squat, bench press, deadlift, overhead press)
- Primary sport and training goals
- Training experience level and years of training
- Equipment access (full gym, home gym, minimal, bodyweight only)
- Weekly training availability (days per week, hours per session, preferred training days)

Training Data: As you use the Service, you create and log:

- Workout sessions (date, time, exercises performed)
- Exercise performance (sets, reps, weight, RPE)

- Training programs (phases, exercises, prescriptions)
- Season calendars (sport, dates, priority levels)
- Competitions and key events (name, date, type, priority)
- Morning check-ins (body weight, resting heart rate, sleep hours, sleep quality, soreness level, energy level, mood)

Coach-Athlete Relationships: Coaches and athletes connected via coach codes establish data-sharing relationships where:

- Athletes grant coaches access to their profiles, workout logs, biometric data, and genetic information
- Coaches can view, but not modify, athlete data
- Athletes can revoke coach access at any time

Payment Information: Payment processing is handled by Stripe. We do not store full credit card numbers. Stripe collects:

- Billing name and address
- Credit card information (processed and stored by Stripe)
- Billing history and transaction records

Communications: We collect information when you:

- Contact customer support (email content, attachments)
- Participate in surveys or feedback requests
- Sign up for newsletters or marketing communications

1.2 Information Collected Automatically

Usage Data: When you access the Service, we automatically collect:

- IP address
- Browser type and version
- Device type and operating system
- Pages visited and time spent on pages
- Referring website or source
- Date and time of access
- User agent string

Cookies and Tracking Technologies: We use cookies, session tokens, and similar technologies to:

- Maintain user authentication sessions
- Remember user preferences
- Analyze platform usage and performance
- Prevent fraudulent activity

You can control cookie preferences through your browser settings, but disabling cookies may limit functionality.

Audit Logs: For security and compliance purposes, we maintain comprehensive audit logs that record:

- User ID performing each action
- Action type (view, create, update, delete, export)
- Resource type and ID (which record was accessed)
- IP address and user agent
- Timestamp

Audit logs are retained for compliance with FERPA and data protection regulations.

1.3 Information from Third-Party Integrations

Garmin Connect: When you connect your Garmin account, we collect:

- Resting heart rate (daily)
- Heart rate variability (HRV)
- Sleep duration and Garmin Sleep Score
- Body Battery level
- Average daily stress level
- Body weight (from Garmin-connected scales)
- OAuth access tokens and refresh tokens (encrypted)

We sync this data automatically at 6:00 AM and 7:00 PM ET daily, with manual sync available on demand. You may disconnect your Garmin account at any time through account settings.

Perplexity AI: When you generate an AI training plan, we send anonymized training parameters to Perplexity Sonar API:

- Genetic markers (ACTN3/FTO genotypes)
- Physical limitations
- Training goals and experience level
- Equipment access and availability
- Season calendar and competition dates
- 1RM baselines

We do NOT send personally identifiable information (name, email, phone number, address) to Perplexity. The AI service processes only the technical parameters required for plan generation.

2. How We Use Your Information

We use the information we collect for the following purposes:

2.1 Service Delivery

- Create and maintain your account
- Authenticate users and manage sessions
- Provide personalized training programs and exercise recommendations
- Generate AI-powered periodized training plans
- Sync biometric data from Garmin Connect
- Calculate biometric baselines and generate recovery alerts
- Enable coach-athlete roster management
- Display progress charts and performance analytics
- Filter exercises based on physical limitations

2.2 Billing and Subscription Management

- Process subscription payments through Stripe
- Send billing confirmations and invoices
- Manage subscription renewals and cancellations
- Handle refund requests and payment disputes
- Provide access to Stripe Customer Portal for self-service billing management

2.3 Communication

- Send service-related notifications (account creation, password resets, subscription changes)
- Respond to customer support inquiries
- Send biometric alerts when recovery metrics deviate from baselines
- Notify coaches of athlete compliance and alert status
- Provide product updates and feature announcements
- Send marketing communications (with your consent, which you may withdraw at any time)

2.4 Platform Improvement and Analytics

- Analyze usage patterns to improve platform functionality
- Identify and fix bugs and technical issues
- Conduct research and development for new features
- Optimize AI training plan algorithms
- Aggregate and anonymize data for statistical analysis

Monitor platform performance and uptime

2.5 Security and Compliance

Detect and prevent fraudulent activity

Enforce Terms of Service

Maintain audit logs for FERPA compliance

Respond to legal requests and prevent harm

Conduct security assessments and vulnerability testing

Monitor for unauthorized access or data breaches

3. How We Share Your Information

We do not sell, rent, or trade your personal information. We share information only in the following limited circumstances:

3.1 With Your Consent

Coach-Athlete Relationships: When you enter a coach code, you explicitly grant that coach access to:

Your profile information (name, genetic markers, physical limitations, 1RM baselines)

Workout logs and performance data

Biometric data synced from Garmin

Morning check-in responses

Progress charts and analytics

Biometric alerts

You may revoke coach access at any time through account settings.

Organizational Accounts: For athletes in school or university programs, administrators and assigned coaches within your organization may access your training data in accordance with FERPA regulations and the institution's data sharing policies.

3.2 Service Providers (Subprocessors)

We engage trusted third-party service providers to support platform operations:

Stripe: Payment processing, subscription billing, and invoice generation. Stripe's privacy policy governs their handling of payment data: https://stripe.com/privacy

Perplexity AI:AI-powered training plan generation. We send only anonymized training parameters (no personally identifiable information). Perplexity's privacy policy: https://www.perplexity.ai/privacy

Vultr: Infrastructure hosting on dedicated VPS servers with encrypted data storage. Vultr's privacy policy: https://www.vultr.com/legal/privacy/

All service providers are contractually obligated to protect your information and use it only for the purposes we specify.

3.3 Legal Obligations

We may disclose your information when required by law or in response to:

- Valid legal process (subpoenas, court orders, warrants)
- Governmental or regulatory requests
- Investigations of potential violations of our Terms of Service
- Protection of our rights, property, or safety, or that of our users or the public
- Detection and prevention of fraud, security breaches, or technical issues

For educational accounts subject to FERPA, we will comply with lawful requests for student records and notify the institution unless prohibited by law.

3.4 Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of assets, your information may be transferred to the successor entity. We will provide notice before your information becomes subject to a different privacy policy.

3.5 Aggregate and Anonymized Data

We may share aggregated, de-identified, or anonymized data that cannot reasonably be used to identify you:

- Industry research and benchmarking reports
- Platform usage statistics
- Anonymized training trends and outcomes
- Academic research collaborations (with institutional approval for educational accounts)

4. FERPA Compliance (Educational Institutions)

When StriveSumma is used by schools or universities receiving federal funding, student-athlete data may constitute education records protected under the Family Educational Rights and Privacy Act (FERPA).

4.1 School Official Exception

We act as a "school official" with legitimate educational interests when processing student data on behalf of educational institutions. This permits us to access student records without prior consent for the purpose of providing athletic training services.

4.2 Data Processing Agreement

Educational institutions execute a Data Processing Agreement (DPA) with us that specifies:

- Scope and purpose of data access
- Permitted uses of student data (limited to athletic training services)
- Prohibition on re-disclosure without institutional consent
- Data security and encryption requirements
- Data retention and deletion timelines
- Breach notification procedures (24-48 hours)
- Annual security assessments
- Audit rights and compliance verification

4.3 Student Data Protection Commitments

For educational accounts, we commit to:

- **No Advertising:** We do not use student data to target advertisements
- **No Profiling:** We do not create marketing profiles based on student data
- **No Sale of Data:** We do not sell student information to third parties
- **Limited Collection:** We collect only data necessary for athletic training services
- **Purpose Limitation:** Student data is used solely for providing the Service to the institution
- **Transparent Subprocessors:** All third-party processors are disclosed in the DPA

4.4 Student and Parent Rights

Students (or parents/guardians for students under 18) have the right to:

Access: Request a copy of all data we maintain about the student within 45 days of the request. Data can be exported via the Settings page in CSV format.

Amendment: Request correction of inaccurate or misleading data. Students and authorized school personnel can edit profile information, check-ins, and workout logs directly through the platform.

Deletion: Request deletion of data when it is no longer needed for educational purposes or upon graduation/departure from the institution. Deletion requests are processed within 45 days.

Breach Notification: Receive timely notice of any data breach affecting the student's education records, including the nature of the breach, compromised data, remediation steps, and contact information for further inquiry.

4.5 Institutional Controls

Administrators at educational institutions have access to:

- Organization-level settings and user provisioning
- Audit logs showing all access to student records
- Data export tools for compliance verification
- Roster management (add/remove coaches and athletes)
- Retention policy configuration
- Bulk data deletion upon contract termination

5. Data Security

We implement robust technical and organizational measures to protect your information:

5.1 Encryption

Data in Transit: All communication between your device and our servers is encrypted using TLS 1.2 (Transport Layer Security). We enforce HTTPS for all connections and implement HTTP Strict Transport Security (HSTS) headers.

Data at Rest: Sensitive data stored in our PostgreSQL database is encrypted using:

- PostgreSQL pgcrypto extension for encryption at rest
- Fernet AES-128-CBC encryption for Garmin OAuth credentials
- Bcrypt hashing for passwords (never stored in plain text)

5.2 Access Controls

- **Role-Based Access Control (RBAC):** Users have access only to data appropriate to their role (Athlete, Coach, Administrator)
- **Multi-Tenant Isolation:** Organization boundaries prevent cross-institution data access

Row-Level Security: Coaches can access only athletes explicitly assigned to them

Session Management: Secure session tokens with configurable expiration

Authentication: Better Auth framework with support for multi-factor authentication (MFA)

5.3 Infrastructure Security

Dedicated VPS Hosting: Our application runs on a dedicated Vultr VPS server (no shared hosting) with:

UFW (Uncomplicated Firewall) configured to allow only necessary ports (22, 80, 443)

Fail2ban for intrusion detection and automatic IP blocking

SSH key-only authentication (password login disabled)

No root password login

Regular security updates and patch management

Internal Service Isolation: The Garmin sync microservice (Python FastAPI) communicates only over localhost and is never exposed to the internet. External requests cannot directly access the sync service.

Web Server Security: Nginx reverse proxy with security headers:

X-Frame-Options: DENY (prevents clickjacking)

X-Content-Type-Options: nosniff (prevents MIME sniffing)

X-XSS-Protection: 1; mode=block (blocks cross-site scripting)

Strict-Transport-Security: max-age=31536000 (enforces HTTPS)

Referrer-Policy: strict-origin-when-cross-origin (controls referrer information)

5.4 Audit Logging

We maintain comprehensive audit logs that record every access to user data:

User ID performing the action

Action type (view, create, update, delete, export)

Resource type and ID (which record was accessed)

IP address and user agent

Timestamp

Audit logs are indexed for efficient querying and retained for compliance purposes. Logs are reviewed regularly to detect suspicious activity.

5.5 Monitoring and Incident Response

Continuous server monitoring and uptime tracking

- Automated biometric alert system monitors data access patterns
- 24-48 hour breach notification commitment for educational accounts
- Incident response plan for security events
- Regular vulnerability assessments and penetration testing

5.6 Employee Access

Access to production systems and user data is restricted to authorized personnel on a need-to-know basis. All personnel with access to sensitive data are bound by confidentiality agreements.

5.7 Limitations

While we employ industry-standard security measures, no system can guarantee absolute security. You acknowledge that you provide information at your own risk. We encourage you to use strong, unique passwords and enable multi-factor authentication when available.

6. Data Retention

6.1 Active Accounts

We retain your data for as long as your account is active and you continue using the Service. This includes:

- Account information and profile data
- Workout logs and training programs
- Biometric data synced from Garmin
- Genetic profiles
- Morning check-ins and progress data
- Coach-athlete relationships

6.2 Inactive Accounts

If your account remains inactive (no login) for an extended period, we may contact you to confirm whether you wish to retain your account. Accounts inactive for more than 24 months may be deleted after providing notice.

6.3 Account Deletion

When you request account deletion:

- Personal data, workout logs, biometric data, and genetic profiles are permanently deleted within 30 days
- Anonymized aggregate data may be retained for statistical analysis
- Audit logs required for compliance may be retained as required by law
- Billing records may be retained for tax, accounting, and fraud prevention purposes as required by law (typically 7 years)

6.4 Educational Account Retention

For student-athlete accounts under educational institutions:

During Enrollment: Data is retained for the duration of the student's enrollment and participation in the athletic program.

Upon Graduation/Departure: Data is deleted according to the institution's retention policy, typically within 30-90 days of departure unless the institution requires longer retention for program evaluation or records purposes.

Upon Contract Termination: If the institution terminates its contract with StriveSumma, all student data is deleted within 30 days unless the institution requests a longer transition period (not to exceed 90 days).

Upon Individual Request: Students or parents/guardians may request deletion at any time. Requests are processed within 45 days in accordance with FERPA requirements.

6.5 Backup Retention

Deleted data may persist in encrypted backups for up to 90 days before permanent removal from all systems.

7. Your Privacy Rights

7.1 Access

You have the right to request a copy of the personal information we maintain about you. You can export your data in CSV format directly from the Settings page, or contact us at privacy@strivesumma.com for a comprehensive data report.

7.2 Correction

You may update your profile information, training data, and account settings at any time through the platform. If you identify inaccurate information you cannot correct yourself, contact us for assistance.

7.3 Deletion

You may request deletion of your account and all associated data at any time. Deletion is permanent and cannot be undone. To request deletion, use the account deletion feature in Settings or contact support@strivesumma.com.

7.4 Data Portability

You can export your workout logs, biometric data, genetic profiles, and training programs in CSV format from the Settings page. We will provide data in a structured, commonly used, machine-readable format.

7.5 Withdraw Consent

Garmin Integration: You may disconnect your Garmin account at any time, which stops future data synchronization. Previously synced data will be retained unless you request deletion.

Coach Access: You may revoke coach access at any time through account settings. Upon revocation, the coach will immediately lose access to your data.

Marketing Communications: You may opt out of marketing emails by clicking the unsubscribe link in any marketing message or updating your communication preferences in account settings.

7.6 Additional Rights for EU/UK Residents (GDPR)

If you are located in the European Union or United Kingdom, you have additional rights under the General Data Protection Regulation (GDPR):

- **Right to Restriction:** Request that we limit processing of your data in certain circumstances
- **Right to Object:** Object to processing based on legitimate interests
- **Right to Lodge a Complaint:** File a complaint with your local data protection authority

Legal Basis for Processing: We process your data based on:

- **Contract Performance:** To provide the services you subscribed to
- **Consent:** For Garmin integration, genetic data processing, and marketing communications
- **Legitimate Interests:** For platform improvement, security, and fraud prevention
- **Legal Obligation:** For compliance with FERPA, tax laws, and legal requests

7.7 California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

Right to Know: Request disclosure of the categories and specific pieces of personal information we have collected about you in the past 12 months.

Right to Delete: Request deletion of your personal information, subject to certain exceptions.

Right to Opt-Out of Sale: We do not sell personal information. If our practices change, we will provide a "Do Not Sell My Personal Information" link.

Right to Non-Discrimination: We will not discriminate against you for exercising your privacy rights.

Shine the Light: Request information about disclosure of personal information to third parties for their direct marketing purposes (we do not engage in such disclosures).

To exercise your California privacy rights, contact us at privacy@strivesumma.com or call our toll-free number (to be established for California users). We will verify your identity before processing requests.

7.8 Exercising Your Rights

To exercise any of these rights:

- Use the self-service tools in account Settings (export, deletion, profile updates)
- Email privacy@strivesumma.com with your request
- For educational accounts, contact your institution's administrator

We will respond to verified requests within 30 days (45 days for FERPA requests). We may request additional information to verify your identity before fulfilling requests.

8. Children's Privacy

8.1 Age Requirements

StriveSumma is not intended for children under 13 years of age. We do not knowingly collect personal information from children under 13 except through COPPA-compliant educational accounts.

8.2 Parental Consent

Users between 13 and 18 must have parental or guardian consent to use the Service. By creating an account for a minor, parents/guardians represent that they have the authority to consent on behalf of the minor.

8.3 Educational Accounts Under 13 (COPPA Compliance)

When educational institutions serve athletes under 13, they act as the parent's agent and provide consent on behalf of parents under the school official exception. Institutions must:

- Notify parents of the Service and data collection practices
- Provide parents with access to their child's data
- Allow parents to request deletion of their child's data
- Obtain verifiable parental consent where required by COPPA

8.4 Discovery of Underage Accounts

If we discover that we have collected personal information from a child under 13 without proper consent, we will delete the account and all associated data immediately.

9. International Data Transfers

StriveSumma is based in the United States. Your information is stored on servers located in the United States (Vultr data centers).

If you access the Service from outside the United States, you acknowledge that your information will be transferred to, stored in, and processed in the United States, where data protection laws may differ from those in your jurisdiction.

For users in the European Union or United Kingdom, we rely on Standard Contractual Clauses (SCCs) and implement appropriate safeguards to protect your data during international transfers.

10. Third-Party Links

The Service may contain links to third-party websites, services, or resources (e.g., Garmin Connect, Stripe Customer Portal, Perplexity AI). We are not responsible for the privacy practices or content of these third parties. We encourage you to review the privacy policies of any third-party services you access.

11. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or business operations.

We will notify you of material changes by:

- Posting the updated Privacy Policy with a new "Last Updated" date
- Sending email notification to your registered email address
- Displaying a prominent notice on the Service

Your continued use of the Service after the effective date of the revised Privacy Policy constitutes acceptance of the changes. We encourage you to review this Privacy Policy periodically.

12. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

Sheepdog Design Studio LLC Bay Village, Ohio, United States

Email:

General inquiries: privacy@strivesumma.com

Customer support: support@strivesumma.com

Legal inquiries: legal@strivesumma.com

Data Protection Officer (for GDPR/FERPA inquiries): Email: dpo@strivesumma.com

For educational institutions, administrators may also contact their designated account manager or institutional support contact.

We will respond to all inquiries within 30 days (45 days for FERPA-related requests).

Acknowledgment

By using StriveSumma, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy and our Terms of Service.

For educational accounts subject to FERPA, institutional administrators acknowledge that they have reviewed this Privacy Policy and confirm it meets their institution's data protection and student privacy requirements.