

Data Retention and Deletion Policy

Smagpie LLC · Version 1.0 · Effective 2026-09-15 · Public document

Owner	Peter Galbraith, Founder and Data Protection Officer (DPO) — dpo@smagpie.com
Applies to	Smagpie Coaching: the web app (app.smagpie.com), the Session Tracker (track.smagpie.com), the API, the marketing site (smagpie.com), support and billing
Published at	https://smagpie.com/trust/data-retention-policy.pdf
Review	At least annually. Last reviewed 2026-09-15; next review due 2027-09-15
Related	Privacy Policy (smagpie.com/privacy) · Parents' Bill of Rights · Written Information Security Program · Incident Response Plan · SDPC National Data Privacy Agreement

1. Purpose and scope

Smagpie keeps personal data only as long as it is needed to coach athletes, run the service and meet legal obligations. This policy states, for every category of data we hold, why we hold it, how long we keep it, what starts the clock and how it is destroyed. It is the written data retention policy required by the Children's Online Privacy Protection Rule (16 CFR § 312.10, as amended in 2025) and is written to meet the retention and disposition expectations of FERPA school-official arrangements, New York Education Law § 2-d and Part 121, the SDPC National Data Privacy Agreement (Article IV), the GDPR, the CCPA/CPRA, the LGPD and Washington's My Health My Data Act.

Scope. All personal data Smagpie LLC processes for Smagpie Coaching, whether as a controller (coaches, account holders, billing contacts, website visitors, subscribers) or as a processor for a school, district, club or coach (athlete data under the coach-as-controller model in our Privacy Policy). It covers production systems, backups, logs and copies held by service providers under data-processing agreements, but not data held by device vendors (Garmin, Coros, Strava, Intervals.icu) under the athlete's own vendor account, or data on a user's own devices.

Principles. (1) No personal data is kept indefinitely: every category has a maximum period and a trigger. (2) Deletion is the default when the purpose ends; keeping data longer needs a legal basis named in section 6. (3) Data about minors (athletes aged 13–17) is never kept longer than the same data about adults, and Smagpie does not create accounts for children under 13. (4) One schedule: the Privacy Policy, the /trust page and our data-privacy agreements summarize this document; where they differ, this document governs.

2. Definitions

- **Personal data** — information that identifies or can reasonably be linked to a person ("personal information" under COPPA and the CCPA).
- **Minor data** — personal data of an athlete aged 13 to 17.
- **Education record / student data** — personal data about a student that Smagpie holds on behalf of a school or district, including training and activity data rostered under a school team.
- **Retention period and trigger** — the maximum time a category is kept, and the event that starts that clock.
- **Soft-delete window** — the 30 days after a deletion request during which the account is disabled but the request can still be cancelled.
- **Hard delete** — irreversible destruction of records from production systems.
- **Destruction certificate** — the signed PDF issued when a hard delete completes, listing what was destroyed.
- **Backup** — an encrypted, restore-only copy of the production database kept for disaster recovery.
- **Legal hold** — a documented suspension of scheduled deletion for specific records because of a legal obligation or dispute.
- **Pseudonymize** — replace a person's identifiers in a record with a reference that identifies nobody once the account is gone.

3. Retention schedule

Section 3.1 is the schedule published in our Privacy Policy; section 3.2 covers the compliance and operational records behind it. "Deletion request" means a request made through any route in section 7. Minor data follows the same periods.

3.1 Data you give us or create by using the service

Category and purpose	Retention period	Trigger	Deletion method
Account data — name, email, role, profile image, settings. <i>To operate the account and identify you to your team.</i>	Duration of the account + 30 days	Deletion request	Hard delete of the account and every record keyed to it (section 4); image deleted from cloud storage
Team and roster data — memberships, groups, invitations. <i>To run the team you belong to.</i>	Duration of the account + 30 days	Deletion request	Hard delete with the account; invitations and approvals others rely on are kept, pseudonymized
Workout definitions and training plans. <i>To deliver the coaching the athlete and coach agreed to.</i>	Duration of the account + 30 days	Deletion request	Hard delete; content shared into a public library or another team's plan is transferred to the platform without personal data
Activity data — GPS, heart rate, power, pace, perceived exertion, session metrics, activity (.fit) files. <i>To show results, compliance and training load.</i>	Duration of the account + 30 days	Deletion request	Hard delete of database records; activity files deleted from cloud storage
Device integration tokens — Garmin, Coros, Strava, Intervals.icu. <i>To sync with a device the athlete chose to connect.</i>	Until disconnected, or until the account is deleted	Athlete disconnects the device, or deletion request	Token revoked at the vendor and deleted — on day 0 of a deletion request
Billing and transaction records. <i>Tax, accounting and dispute obligations.</i>	7 years after the transaction	Transaction date	Automated purge once 7 years have passed; purchaser reference pseudonymized when the account is deleted
Server logs (anonymized). <i>Security monitoring and debugging.</i>	90 days	Log entry written	Automatic rolling deletion
Support correspondence — email, contact-form and inquiry submissions. <i>Quality of service and follow-up.</i>	2 years after resolution (contact-form submissions: 2 years after receipt)	Resolution / receipt	Automated purge (contact forms) and mailbox retention rules
Audit log events — sign-ins, privileged actions, exports, deletions, consent. <i>Accountability and district audit rights.</i>	1 year (minimum); purged after 1 year unless on legal hold	Event recorded	Daily automated purge of events past the retention period

3.2 Compliance and operational records

Category and purpose	Retention period	Trigger	Deletion method
Consent and age-verification records — the timestamp age verification passed, coach consent certification. <i>Proof of lawful onboarding; birth month and year are never stored.</i>	Duration of the account, then archived on the deletion record for 7 years	Deletion request	Consent row deleted with the account; snapshot kept on the deletion record, which is linked to no live account
Deletion records and destruction certificates. <i>Proof that a deletion happened and what it covered.</i>	7 years after the deletion completes	Deletion completed	Personal snapshots erased and certificate deleted after 7 years; download links expire after 90 days and are re-issued on request
Data export archives — self-service copies of an account's data. <i>Portability.</i>	7 days	Export generated	Download link expires and the archive is removed from storage; deleted at once when the account is deleted
Mailing-list subscriptions — coach and district notice lists. <i>Service-provider change notices you asked for.</i>	Unconfirmed: 30 days. Confirmed: until you unsubscribe	Subscription / unsubscribe	Unconfirmed rows purged daily; an unsubscribed address is kept only as a suppression record and erased on request
AI-assisted authoring records — prompts and generated drafts a coach asked for. <i>Quota, abuse prevention and provenance.</i>	90 days	Record created	Weekly automated purge
Encrypted database backups. <i>Disaster recovery.</i>	Daily copies 7 days; weekly 4 weeks; monthly 5 months. A deleted record is out of every backup within 6 months	Backup taken	Automatic expiry and pruning (section 5)

Website analytics are aggregated and contain no personal data; they are outside this schedule.

4. Deletion process

Every account deletion — self-service, school-initiated or support-initiated — runs through one automated pipeline.

1. **Request (day 0).** A valid request (section 7) creates a deletion record. **The account is disabled immediately:** no sign-in, and nothing new is recorded. Every connected device is disconnected and its token revoked at the vendor, so no later sync can land. A complete copy of the account's data is emailed to the athlete (link valid 7 days), and the athlete — and the requester, if different — is told the scheduled deletion date.
2. **Soft-delete window (days 1–30).** The request may be cancelled: a self-requested deletion by the athlete (signed link in their email), the head coach or Smagpie support; a school-requested deletion by the head coach or support only. Cancelling restores only what was active before. A school may ask support for a shorter window (at least one day).
3. **Hard delete (day 30).** An automated job inventories every record about to be destroyed, records the count and a cryptographic hash, destroys the database records in one transaction, deletes activity files, the profile image and any export archive from cloud storage, and clears caches. Records that must survive (billing, audit log entries, invitations and approvals others depend on) are pseudonymized: the account reference is removed and any stored email is rewritten to a placeholder that identifies nobody.
4. **Destruction certificate.** The requester receives a signed PDF listing the destroyed records by table, the outcome of each vendor token revocation (an unreachable vendor is printed as "not revoked"), the inventory hash and an HMAC-SHA256 signature. Certificates are retained 7 years and re-issued on request to compliance@smagpie.com.
5. **Contract end (schools, districts, clubs).** On written notice, Smagpie support deletes the whole team — every athlete and coach account — through the same pipeline and issues a team-level certificate listing each account's certificate. Destruction completes within 60 days of the notice (sooner on request), consistent with Article IV of the SDPC National DPA.
6. **Removal and dormancy.** Removing an athlete from a team group, or deactivating the account, does not delete it. An account that has received no workout assignments, imported no workouts and not been signed in to for 24 months is treated as abandoned: the head coach is notified, and the account is scheduled for deletion 30 days later unless the coach overrides. This check runs at least quarterly.
7. **Children under 13.** If we learn we hold personal data of a child under 13, we delete it promptly, without the 30-day window, and tell the parent or school where we can.

5. Backup handling

- The production database is dumped nightly and encrypted on the server (AES-256, client-side, using restic) before any copy leaves it. Copies live in a dedicated cloud storage account in the United States (geo-redundant), with a provider separate from the production servers, under credentials the application does not hold.
- Retention tiers — daily copies for 7 days, weekly for 4 weeks, monthly for 5 months — are enforced automatically. Expired copies are pruned and the storage account's 14-day soft-delete window then elapses, so a record hard-deleted from production is absent from every backup within 6 months. Local staging copies on the server's encrypted volume follow the same tiers.
- Backups are restore-only: used for disaster recovery and, on a ticketed request within the retention window, to reverse a deletion made in error — never to reinstate certified-destroyed data except at the written request of the person or school who requested the deletion.
- After any disaster-recovery restore, deletions completed after the restored snapshot are re-applied from the retained deletion records before the service returns to use, so that certified deletions stay deleted.
- Files in cloud storage (activity files, images, exports, certificates) are geo-redundant but not separately backed up; a deleted file is recoverable through the 14-day storage soft-delete window and then gone.

6. Legal holds and retention exceptions

Scheduled deletion is suspended only for the records, and for the period, that an exception requires. Exceptions never widen the categories collected.

Exception	What is retained	How long	Basis
Tax and accounting	Billing and transaction records (pseudonymized after account deletion)	7 years after the transaction	Federal and state tax record-keeping
Active litigation, regulatory inquiry or lawful request	The specific records identified in a written legal-hold notice	Until the matter closes and the DPO releases the hold	Legal obligation; preservation duties
Security incident investigation	Logs and audit events relevant to the incident	Until the post-incident review closes (Incident Response Plan)	Legitimate interest in security
Proof of compliance	Deletion records, destruction certificates, consent snapshots	7 years after the deletion	Accountability to schools, parents and regulators

Only the DPO places or releases a legal hold, recording its date, scope and basis. Deletion requests a hold covers are deferred and the requester is told where the law allows. Holds are reviewed quarterly and released as soon as the basis ends.

7. Deletion requests from athletes, parents and schools

Who	How to ask	What happens
Athlete or coach (own account)	Account page → <i>Delete my account</i> (password and typed name), or privacy@smagpie.com	Immediate disable, data copy emailed, hard delete after the 30-day window
Head coach or school (an athlete on the roster)	Coach roster → <i>Delete account</i> (coach's password, athlete's name, reason), or compliance@smagpie.com	Same pipeline; the athlete is told the school asked and receives their data copy on day 0
Parent or guardian of a minor athlete	Ask the school or club first — it is the controller of the athlete's data — or write to privacy@smagpie.com	For a school-rostered athlete we act on the school's instruction and tell the parent whom to contact. For a club or individually coached athlete we verify the parent and act directly
District or organization (contract end, Part 121 or DPA request)	compliance@smagpie.com , quoting the agreement	Team deletion (section 4, step 5) with a team-level certificate

Verification. In-app requests are verified by password and typed name; email requests against the account's registered address or the school's designated privacy contact, with the ticket reference recorded on the deletion record and certificate.

Timelines. We acknowledge within one business day, disable the account as soon as the request is accepted, complete the hard delete within 30 days of a valid request (45 days where the CCPA allows an extension, with notice) and within 60 days of a contract-end notice, and issue the certificate on completion. Records under section 6 are the only exception, and we say so in the acknowledgement. Access, correction and export are available in the app at any time. Every request and its outcome is recorded in the audit log.

8. Review, ownership and enforcement

The DPO owns this policy and reviews it at least annually, and sooner when the service, a service provider or the law changes materially. Each review confirms that the automated purge jobs behind section 3 ran, that the Privacy Policy, the /trust page and the DPA exhibits still match this schedule, and that any legal holds are still justified; it is recorded in the revision history. Changes that lengthen a retention period or reduce a right are announced at least 30 days in advance, as the Privacy Policy promises.

Questions: privacy@smagpie.com (individuals) · compliance@smagpie.com (schools and districts) · security@smagpie.com (security) · dpo@smagpie.com (Data Protection Officer).

Approval — Approved by Peter Galbraith, Founder and Data Protection Officer, Smagpie LLC.
Signature: Peter Galbraith · Date: 2026-09-15

Revision history

Version	Date	Author	Change
1.0	2026-09-15	P. Galbraith (DPO)	Initial policy