

Privacy Policy

Effective date: October 25, 2026

Sculpt is operated by Jacob Lagesse, based in California, USA. This policy covers the Sculpt app, website and related support. For privacy questions or requests, email sculpt.app.support@gmail.com or write to Jacob Lagesse, 655 Bonanza Ct, Sunnyvale, CA 94087, USA.

Sculpt uses AI body analysis and personalized workout planning to guide adult fitness. This policy explains the data handled by the app and its services.

Account and fitness data

Supabase processes your account identifier, sign-in details, questionnaire answers (including birth date, gender, measurements, activity and goals), scan results and explanations, dated weights, and saved routines, private custom exercises and workout logs to operate and synchronize your account. Apple or Google provides the identity information you choose to share when signing in. We use your birth date to check adult eligibility and derive age for estimates.

Body scan photos and AI

Full body scan photos are stored privately on your device, excluded from backups and app exports. Before upload, Sculpt crops above the shoulders, masks any detected faces remaining in the crop and removes photo metadata. With your explicit permission, cropped photos and relevant age, gender, height, weight, activity, physique goals, approximate outline dimensions, saved scan results and recent workout history are sent through Supabase to OpenAI for photo guidance and analysis. AI workout generation uses your selected days and duration, goals, training experience, muscle preferences, comparable historical muscle scores and trends, recent exercise performance and preferences, and relevant exercise catalog entries. Generating a new routine from these inputs does not upload photos; importing an existing routine sends images as described below. Sculpt does not add your name, email or full birth date to these AI prompts. Photo cropping reduces identifiability but cannot guarantee anonymity.

Importing workout routines

When you choose Read my routine in Import your routine, up to seven selected workout screenshots or photos are sent through Supabase to OpenAI to extract exercise names, workout days, weights, sets and repetitions and match movements against relevant exercise-library entries. Sculpt resizes and re-encodes these images to remove source metadata. Unlike body scan uploads, routine-import images are not automatically cropped above the shoulders or masked for faces: the full selected image content is sent, including any names, faces, messages or other personal information visible in it. Crop out unrelated information and only upload content you have permission to share. Sculpt does not add your account name or email to the import prompt, but cannot remove information visible in the image for you. Source images are held temporarily for import and are not saved in your Sculpt cloud account; the extracted draft and saved routine may be retained.

AI permission and retention

Sculpt asks for explicit AI data-sharing permission before onboarding and a new subscription. If you do not agree, setup does not continue. Your agreement is saved for your account on this device. Future scans, routine imports and AI plans run when you request them. You can stop making AI requests or delete your account in Profile & settings to end use of the service. This does not undo prior processing or cancel Apple billing. Contact support for questions or requests about previously processed data. This permission is separate from the analytics described below. Cropped scan photos and routine-import images are temporary backend request inputs rather than stored in a Sculpt cloud photo library. Imported routine drafts and routines you save can be retained with your account, but do not contain the source images. Provider retention, security and safety policies still apply; Sculpt does not claim Zero Data Retention. OpenAI requests disable stored responses, which does not eliminate all provider retention. Review [OpenAI data controls](#) and [Supabase privacy information](#).

Subscriptions

Apple handles App Store payment information. RevenueCat processes your Sculpt account identifier, purchase and entitlement details, and technical purchase information to validate access and restore subscriptions. Sculpt does not receive your card details. See [RevenueCat privacy information](#).

Sign-in provider information

Google Sign-In may also process device identifiers, sign-in usage and diagnostic information, and approximate region inferred from network information under [Google's privacy policy](#). Sculpt does not request phone-number or location scopes. Apple sign-in is governed by [Apple's privacy information](#). Provider SDK privacy declarations are included in the app bundle.

Analytics and diagnostics — PostHog

We use PostHog to understand how Sculpt is used, improve onboarding and paid features, measure reliability and troubleshoot errors. The app can send app-launch and sign-in events, onboarding step names and time spent, scan/import success or failure events, routine actions and limited routine settings such as training-day counts and duration, and payroll, purchase and restore events. PostHog may receive app/device and operating-system information, anonymous device identifiers, crash reports and technical logs. After sign-in, events can be associated with your Sculpt account UUID. Our backend also sends AI operation metadata such as model, token counts, latency and request identifiers, and RevenueCat subscription lifecycle metadata such as product, renewal/cancellation status and reported purchase amounts. These analytics event payloads exclude body and routine images, AI prompts and response bodies, individual scan scores, height, body weight, names and email addresses. Session replay, automatic screen-view capture and automatic element-interaction capture are disabled. Analytics is used for product improvement and diagnostics, not targeted advertising. See [PostHog privacy information](#).

Analytics retention and deletion

PostHog records follow the retention settings configured for the applicable analytics, logs and diagnostic services. Signing out or deleting your Sculpt account resets the app's local analytics identity; this alone does not delete records PostHog already received. Historical PostHog records require separate deletion and are not currently erased automatically by Sculpt's account-deletion flow. Contact sculpt.app.support@gmail.com to request removal of retained account-linked analytics. Analytics is separate from AI processing; contact support about retained analytics and data requests.

Use and sharing

These providers process data to deliver authentication, storage, purchases, analytics, diagnostics and the AI features you request. Sculpt does not sell fitness data, use it for targeted advertising, or request advertising tracking access. Services also process technical request information, such as IP addresses, for delivery, security and abuse prevention. Third-party services have their own retention and privacy terms; contact support with questions about your data. Service providers receiving Sculpt data must protect it consistently with this policy and applicable data-protection obligations. We do not authorize use of the fitness data we send for advertising.

Storage and deletion

Custom exercises are private to the account that creates them and are not shared with other users. Account-linked profile, custom exercises, scan results and training history remain until you delete them or your account. Progress → Saved scans lets you remove individual scans or their local photos. Profile & settings → Delete account removes your profile and starts deletion of associated backend data, authentication, Apple sign-in authorization and RevenueCat customer records. Cleanup retries if a provider is unavailable; RevenueCat deletion may finish asynchronously. Minimal private deletion-job records are retained to complete and audit erasure. Deleting your account does not cancel Apple billing; cancel through Apple subscription settings. Signed-out account caches on other devices are not remotely erased from those devices; they are protected locally and removed when that device processes account deletion or you remove the app.

Device storage and security

Sensitive local databases and scan photos are excluded from backups. Requests use HTTPS; backend access is scoped to authenticated accounts. No security or anonymization method is perfect.

Adults and policy updates

Sculpt is intended for adults aged 18 and over and is not a medical service. Updates to data-sharing purposes require updated permission where applicable. For data questions, use Help & support in the app.

Contact Sculpt

For support, privacy requests or questions about this policy, email sculpt.app.support@gmail.com. Include your app version and a description of the issue. Do not email body photos, passwords, payment details or identity documents. Account deletion is available directly in the app; no support email is required to delete your account.

Website visits

The public website has no account form or advertising trackers added by Sculpt. GitHub Pages may process your IP address and ordinary request information to serve and secure the site, as described in GitHub's privacy statement. Emailing support sends your message through your email provider and our Google-hosted mailbox. External links lead to services with their own privacy practices.

Your privacy rights

Depending on your location and applicable law, you may have rights to know or access the information we hold; obtain a copy or portable record; correct information; request deletion; restrict or object to processing; withdraw consent; and appeal a decision about a request. You may also complain to your local privacy regulator. California residents may have rights under applicable California privacy laws, including protection against unlawful discrimination for exercising their rights.

Send requests to sculpt.app.support@gmail.com, with enough information to identify your Sculpt account and the request. We use proportionate identity verification and handle authorized-agent requests where required. We respond within applicable legal deadlines, explain permitted extensions or refusals, and provide available appeal information. A paid subscription is not required to exercise privacy rights. To appeal, contact the same email with "Privacy appeal" in the subject. An app export may cover only device data; contact us for a broader account-data request.

Legal bases and international processing

Where a legal basis is required, we rely on performance of our agreement for necessary account and requested services; legitimate interests in operating and securing the service and responding to requests, balanced against your rights; compliance with legal obligations; and consent where required. Sensitive health-related processing also requires an applicable additional legal condition, including explicit consent where required.

We operate in the United States. Providers may process information in the United States and other countries, whose privacy laws may differ from yours. Where applicable law requires transfer safeguards, transfers are subject to those requirements, such as an applicable adequacy decision or approved contractual safeguards. Contact us for information about recipients, processing locations and safeguards relevant to your information, or to request an available copy of the applicable safeguard.