PRIVACY POLICY

Swimka Mobile Application & Website

Effective Date: 18th November 2026

1. WHO WE ARE

Swimka ("App," "we," "us," "our") is operated by SSO Active, a Société par Actions Simplifiée (simplified joint-stock company) incorporated and organized under the laws of France, registered with the RCS of Evry under number 810 963 306.

Legal Address:

12 rue Fernand Léger, 91440 Bures-sur-Yvette, France

Contact Email:

contact@openswim.fr

Jurisdiction-Specific Note:

Under this Privacy Policy, SSO Active serves as the "data controller" for purposes of European data protection law (GDPR, UK GDPR, French CNIL regulations) and the "business" for purposes of U.S. state privacy laws (CCPA, CPRA, VCDPA, TDPSA, CTDPA, and similar laws).

This Privacy Policy is part of our Terms of Service and is incorporated by reference. By accepting the Terms of Service, you also accept this Privacy Policy. In the event of conflict, this Privacy Policy will prevail. Terms capitalized but not defined herein have the meaning ascribed to them in our Terms of Service. This Privacy Policy explains how we use your personal information.

Swimka is committed to protecting your privacy and maintaining transparency regarding how we collect, use, and protect your personal information. This comprehensive Privacy Policy describes our practices in detail and is designed to help you understand your rights and make informed decisions about your personal data.

Which App This Policy Covers: This Privacy Policy covers the new Swimka app (version 6 and later) and our website. Earlier versions of the App, including the current Android app, remain covered by the previous Privacy Policy. The features available to you depend on the version of the App you use and may change over time. Where this Policy describes a feature that your version does not offer, that part does not apply until it does.

2. WHERE YOU LIVE MATTERS

This Privacy Policy applies globally to all users of the Swimka App and Website, regardless of location. However, privacy laws vary by region, and your rights depend on where you reside. Swimka recognizes that privacy is a fundamental right and that different jurisdictions have established varying levels of legal protection for personal information. We aim to apply a high standard of privacy protection globally, while recognizing that rights and obligations vary by jurisdiction:

- If you are located in the European Union, the United Kingdom, or any other jurisdiction where the GDPR or similar data protection laws apply: You enjoy comprehensive privacy rights including access, rectification, deletion, portability, and the right to lodge complaints with a supervisory authority. These rights are described in Section 10.1.
- If you are located in California, Colorado, Connecticut, Utah, Virginia, Texas, or any other U.S. state with privacy laws: You may have rights to know, delete, correct, and opt out of certain data uses and sharing. These rights are described in Section 10.2. We recommend reviewing the state-specific language applicable to your location.
- If you are located elsewhere: You may have privacy rights under your local laws. Please contact us to understand what rights may apply to you (contact@openswim.fr).

3. PERSONAL INFORMATION WE COLLECT

We collect personal information from three primary sources: (1) information you directly provide to us, (2) information we collect automatically, and (3) information we receive from third parties. This section provides a comprehensive overview of all categories of personal information that we process in connection with the Swimka application and website. Understanding what data we collect helps you make informed choices about

your privacy and exercise your rights effectively. We have organized this information by source and type to provide maximum transparency.

3.1 Information You Provide to Us

The following categories of information are collected when you create an account, set up your profile, or interact with Swimka features:

Account Registration & Profile Information:

- Name, email address
- Gender, date of birth, city/location
- Body measurements (weight, height)
- Photograph (optional; used for profile avatar)
- Swimming experience level (beginner, intermediate, advanced)
- Swimming discipline preferences (pool, open water, triathlon, etc.)
- Annual swimming goals and weekly training targets
- Reasons for swimming, other sports you do, and the equipment you use
- Your confirmation that you are 18 or over, and the date you gave it
- Your FFN license number, if you are in France and choose to add it
- Notification preferences and communication settings
- Language and display settings

Life-Stage Information (optional):

- Whether you are pregnant, postnatal or going through menopause, if you choose to answer our life-stage questions, and the date your answers are due for review

Bubble and Other AI Features:

- Your conversations with Bubble, our AI swim coach, including anything you tell her about your training, injuries, health or life stage
- Bubble's notes about you between conversations (her “memory”), which you can read and clear in My Account
- Your AI permissions and settings, and your credit balance and use
- Content the AI features create for you, such as your training plan and the daily comment on your home screen

Clubs and Partners:

- The Clubs you follow and, where a Club offers it, whether you chose to share your contact details with its partner
- Which partner's link brought you to Swimka, if you joined through one

Permission Records:

- The permissions you give or refuse in the App (for example for Bubble, the life-stage questions, analytics, or sharing with a partner) and your acceptance of the Terms of Service, each with its date and the version of the wording you saw

Account Usage & Personalization: (the community items below apply where your version of the App offers them)

- Account settings and preferences (face ID/touch ID, push notifications, profile visibility)
- Profile status setting (public, partially public, or private)
- Followers and following list (if you set profile to public or semi-public)
- Messages, comments, and communications with other users
- Participation in groups, events, and challenges
- Feedback, reviews, and user support requests

Workout & Activity Data (User-Generated):

- Workout records you create or log (date, time, distance, duration, location, route)
- Performance metrics (speed, pace, splits, heart rate if recorded, calories burned, rest intervals)
- Photos and comments associated with activities

- Favorites, saved workouts, and custom training programs
- Personal bests and achievement records
- Calendar entries and scheduled training sessions

Third-Party Synchronization Data:

When you connect Swimka to external fitness apps and devices (such as Garmin Connect, Apple Health/Apple Watch, COROS, Suunto and Strava, where available), we receive:

- Historical workout data from the last 30 days (or as permitted by the third-party app)
- Activity details: distance, time, speed, heart rate, calories, rest time
- Workout type and sport classifications
- Geolocation data of activities (if shared by third-party service)

3.2 Information Collected Automatically

As you use the Swimka App and Website, we automatically collect certain information about your device, your usage patterns, and your interactions with our platform. This automatic collection occurs even if you do not actively provide information to us and helps us improve our services and detect security issues:

Device & Technical Information:

- Device type and model (e.g., iPhone 15, Samsung Galaxy)
- Operating system and version (iOS or Android)
- App version and build number
- Unique device identifier (we do not collect the advertising identifier)
- Language and localization settings
- Internet connection type

Usage & Navigation Data:

- Pages and features you access within the App
- Frequency and duration of use
- Clicks, interactions, and navigation patterns
- Crash logs and error information
- Search queries within the App
- Which training videos you watch, with playback statistics (through Mux)

Location Data:

- City/region (derived from IP address or profile)
- The App does not read your phone's location; your city is the one you type
- Geolocation of activities during workout tracking (if enabled)

Cookies, SDKs & Similar Technologies: See Section 6 for a complete description of the cookies, SDKs, and tracking technologies used by Swimka, including their purposes, data collected, and opt-out mechanisms.

3.3 Information from Third Parties

In addition to information you provide directly and information we collect automatically, we receive information from external sources. This helps us enhance our services and provide you with better functionality. All information received from third parties is treated with the same care and protection as information you provide directly:

Fitness & Health Platforms:

When you authorize Swimka to connect to a fitness app or device (such as Garmin, Apple Health, COROS, Suunto or Strava), we receive fitness and health data shared through those platforms' APIs.

Service Providers:

Our service providers (described in Section 5) may provide information to us as part of fulfilling contracted services (e.g., customer support data, analytics).

Publicly Available Sources:

If you set your profile to public, other users can view and reference your profile information, activities, and achievements.

Fédération Française de Natation (FFN):

If you add your FFN license, the FFN tells us whether it is valid (see Section 5.1).

4. HOW WE USE YOUR PERSONAL INFORMATION

We process your personal information for the following lawful purposes. Data protection laws require that we have a legal basis for processing your personal information. Swimka has identified multiple legal bases for our processing activities, each explained in detail below. Our approach to data processing is grounded in transparency and respect for your privacy. We only process your data when we have a valid legal basis, and we have carefully balanced your privacy rights against our legitimate interests in each case.

4.1 Performance of Contract & App Functionality

- Creating and maintaining your Swimka account
- Authenticating your identity and verifying account ownership
- Providing app features: workout logging, training programs, performance tracking, community interaction
- Storing and syncing your workout data across devices
- Displaying your profile, activities, and achievements (according to your privacy settings)
- Facilitating connections with other users (followers, groups, events, challenges)
- Processing third-party fitness app integrations (such as Garmin, Apple Health, COROS, Suunto or Strava)
- Providing customer support and resolving account issues
- Linking you to registration for our events on Njuko's platform, where your registration and payment are handled
- Providing AI training plans, the daily comment and Bubble's coaching, once you have given the permissions described in Section 12
- Showing you the Clubs you follow and their content
- Checking your FFN license when you ask us to
- Managing your Subscription and credits, and recording the permissions you give and the version of the Terms of Service you accept
- Looking at a conversation with Bubble when you report a problem with it

4.2 Legitimate Interests

We pursue the following legitimate interests, balanced against your rights and expectations. These legitimate interests are carefully evaluated to ensure they do not override your privacy rights and are communicated transparently so you can understand why we process your data in these ways.

App Improvement & Optimization:

Analyzing usage patterns, feature adoption, and user behavior to identify bugs, improve performance, and develop new features that enhance your experience and the overall quality of the Swimka application. This includes content-free figures about Bubble, such as the number and length of conversations and what they cost. Where analytics tools run on your device, such as Mixpanel, we ask for your consent first if you are in the EU or UK (see Section 6).

Performance Analytics & Insights:

Aggregating and anonymizing workout data to provide users with comparative statistics, trends, and insights (e.g., personal records, seasonal patterns) while protecting individual privacy through anonymization techniques.

Fraud Prevention & Security:

Monitoring for unauthorized access, unusual account activity, and potential misuse to protect your account and the broader community from malicious actors and security threats.

Personalization:

Customizing training recommendations, suggested workouts, and community suggestions based on your fitness level, goals, and activity history to provide a more engaging and relevant user experience.

Community Safety & Content Moderation:

Enforcing community standards, detecting abuse, and managing public content to maintain a safe and respectful environment for all users of the Swimka platform.

Club Statistics for Partners:

Producing anonymous figures about each Club for its partner, such as the number of followers or premium subscribers, or the share of followers with a given level or favorite stroke. Each figure covers at least 10 people and never includes health information, life-stage answers, location or individual swims.

Partner Referrals:

Recording which partner's link brought you to Swimka, so we can see which partnerships work.

Updates:

Sending app updates, feature announcements, and community highlights to keep users informed about developments and opportunities.

4.3 Compliance with Legal Obligations

- Retaining records required by French tax and accounting law
- Responding to lawful requests from law enforcement or government agencies
- Defending against legal claims and dispute resolution
- Compliance with CNIL orders or supervisory authority requests

4.4 Consent

Where required by law, we request your explicit consent for:

- Push notifications and email communications (opt-in during account setup; revocable in settings)
- Precise geolocation tracking (requested at device level and app level)
- Marketing emails
- Bubble: using what you share with Bubble, including any health information, to coach you (explicit consent on Bubble's permission screen)
- Life-stage questions: storing and using your answers about pregnancy, postnatal or menopause (explicit consent when you first answer them)
- Conversation review: letting our team read your conversations with Bubble under a pseudonym to improve her (a separate, optional box on Bubble's permission screen, which you can withdraw at any time in My Account)
- Analytics and attribution: running Mixpanel and Airbridge on your device, if you are in the EU or UK (asked when you first open the App)
- Sharing your contact details with a Club's partner, where a Club offers it (an optional box when you follow the Club)

You may withdraw consent at any time in My Account or Settings in the App, or by contacting us. Withdrawing consent stops future use; it does not affect what we did before.

4.5 Special Category Data

Health Data:

Some information you give us is health information, which the law protects more strictly. We keep it separate from your ordinary training data:

- Training data: your swims (distance, time, pace, strokes), calories and training plans, which we use to provide the App (performance of our contract with you).
- Health information: your life-stage answers, anything you tell Bubble about injuries or your health, which we use only with your explicit consent (Article 9(2)(a) GDPR). You can withdraw it at any time (see Section 10.1 J).

We never share health information with Club partners or use it for advertising or for the daily comment, and Mixpanel and Airbridge never receive it.

Precise Geolocation:

Your precise location during workouts is processed based on your affirmative permission (typically at device level). We do not process precise location for non-fitness purposes without your consent.

4.6 Automated Decision-Making & Profiling

Our AI features (AI training plans, the daily comment and Bubble) make suggestions for you. They do not make decisions that have legal or similarly significant effects on you, such as closing your account or refusing you a service. You can ignore any suggestion, change your goals, switch Bubble off in My Account, or ask a person to review an AI suggestion. Section 12 explains how the AI features work.

5. HOW WE SHARE YOUR PERSONAL INFORMATION

Transparency about data sharing is essential to your understanding of how your information is used. Swimka shares personal information only when necessary to provide our services, comply with legal obligations, or pursue legitimate interests that are balanced carefully against your privacy rights. This section details every category of recipient that may receive your data, the legal basis for each sharing, and your rights regarding those disclosures.

5.1 Categories of Recipients

We share your personal information with the following categories of recipients. Each recipient category is subject to contractual obligations regarding data protection and use restrictions:

Service Providers & Processors:

- Eastern Peak: Backend development, maintenance, and technical support
- Amazon Web Services (AWS): Runs Claude, the AI model made by Anthropic, through its Bedrock service in the EU, for AI training plans, the daily comment and Bubble, and stores Bubble's memory (Paris, France). AWS does not use this data to train AI models and does not share it with Anthropic
- Our AI contractor: An independent contractor who builds and operates our AI service for us, under our instruction in the United Kingdom
- Google Firebase: Push notification infrastructure (FCM) and remote configuration of the App
- Brevo, formerly Sendinblue: Email delivery and marketing automation (data processor acting on our instructions)
- Sentry: Crash and error monitoring, performance tracking
- Airbridge: Mobile attribution and marketing analytics
- Meta / Facebook: SDK functionality, Facebook Login (if you choose to sign in with Facebook), and retargeting ads outside the app
- RevenueCat: In-app purchase and subscription management
- Njuko: Event registration and payment processing for swimming events, on Njuko’s platform
- DigitalOcean: Hosting of our servers and database in Frankfurt, Germany, including Bubble's conversation transcripts, and backups
- Mixpanel: Product analytics, with data held in the EU. Mixpanel receives usage events linked to an account number, never your name, email, city, year of birth, pace, life-stage answers or conversations with Bubble
- Mux: Hosting and streaming of our training videos, with playback statistics (some older videos are still played through YouTube)
- Apple (Apple Maps): Looking up your city from the name you type
- Apple & Google: Payment processing for in-app purchases (note: we do not receive or process your payment card details; Apple and Google handle all payment information)

For each service provider, we maintain contractual arrangements requiring them to: process data only as instructed, maintain appropriate security safeguards, assist with your data rights requests, delete or return data upon contract termination, and notify us of any breaches.

Third-Party Fitness & Health Apps (at your direction):

When you authorize integration with a fitness app or device (such as Garmin, Apple Health, COROS, Suunto or Strava), we share your Swimka workout data with those platforms, and we receive data from them. These integrations are governed by those third parties' privacy policies. You control which integrations are active and can disconnect at any time in your app settings.

Clubs and Partners:

Following a Club does not share your name or contact details with its partner. Partners receive only anonymous figures about their Club, such as the number of followers or premium subscribers, or the share of followers with

a given level or favorite stroke. Each figure covers at least 10 people and never includes health information, life-stage answers, location or individual swims.

Where a Club offers it, and only if you tick the box when following the Club, we share your name and email, and whether you are a Premium member, with the named partner so it can send you news and offers about its events and products. The partner then uses your details under its own privacy policy and must tell you, at the latest in its first message, that it received them from Swimka. You can stop sharing at any time in the Club's settings or by unfollowing the Club, and we will ask the partner to delete your details.

Fédération Française de Natation (FFN):

If you are in France and add your FFN license, we send your license number, first name and last name to the FFN, which confirms whether the license is valid. We keep your license number on your account until you remove it.

Partner Links:

If you joined Swimka through a partner's link, we record which partner's link it was, for our own use. Links to partners' shops on Club pages are plain links: we do not track what you do on the partner's site.

Community & Public Features: Where your version of the App offers community features, the following applies.

Please note that all Users who use the App are displayed on the Leaderboard, and you generally cannot opt out of appearing on the Leaderboard. By using the App, you acknowledge and consent to your username and swimming statistics being visible to other Users through the Leaderboard. While this is a default feature of the App, users located in the European Union and the United Kingdom may request removal from the Leaderboard by contacting us by email. We will assess and process such requests in accordance with our obligations under applicable data protection laws, including GDPR Article 21.

If you set your profile to public or semi-public, the following information is visible to other Swimka users:

- Profile name, profile picture, location (city)
- Public activities, performance metrics, and achievements
- Comments, messages, and group/event participation
- Followers and following list

Legal Requirements & Law Enforcement:

- Government or law enforcement agencies (upon valid legal process, subpoena, or court order)
- Compliance with data privacy authority investigations or data protection authority requests
- Fraud investigations or to protect Swimka against legal liability

Business Transfer:

In the event of a merger, acquisition, bankruptcy, or sale of assets, your personal information may be transferred as part of that transaction. We will provide notice of any such change and any choices you may have.

Auditors & Consultants:

- External auditors (for financial and compliance audits)
- Legal and compliance consultants
- Data protection consultants and DPA advisors

These recipients are contractually bound to confidentiality and use data only for their specified purpose.

5.2 Sharing of Special Categories & Sensitive Information

Your health information (life-stage answers and health information you share with Bubble) and precise geolocation are shared only with:

- Service providers under contractual arrangements (AWS and our AI contractor for the AI features; DigitalOcean and Eastern Peak for hosting and maintenance) with technical and organizational safeguards
- Third-party health apps (such as Garmin, Apple Health, COROS, Suunto or Strava) at your explicit authorization
- Law enforcement (only upon valid legal process)

We do not sell or share health data or precise geolocation for marketing or profit purposes. We never share health information with Club partners, and Mixpanel and Airbridge never receive it.

5.3 Sale or Sharing of Personal Information (CCPA/CPRA Disclosure)

For California and other U.S. state privacy law purposes: We do not “sell” your personal information as defined by CCPA §1798.100 (exchange for monetary consideration).

We partner with third-party advertising and analytics providers, such as Meta and Airbridge, to help us understand how you use our services and to deliver advertisements tailored to your interests. These partners may collect identifiers from your device to facilitate these services. While we do not sell your personal information for monetary compensation, we do use it for these targeted advertising purposes. You can control or opt-out of this tracking through your device settings (such as Apple's App Tracking Transparency feature) or through your browser's ad-tracking controls.

We do disclose your personal information for “business purposes” (CCPA §1798.140(d)) to the following categories:

- Service providers under contract (for analytics, email delivery, cloud services, customer support)
- Third-party fitness integrations (at your authorization)
- Aggregated, de-identified usage statistics (for research and improvement)

If our sale or sharing practices change in the future, we will update this Privacy Policy, provide prominent notice, and implement opt-out mechanisms including a “Do Not Sell or Share My Personal Information” link.

If you ask us to share your contact details with a Club's partner, that is a disclosure you direct, not a sale or sharing by us.

6. COOKIES, SDKs, AND SIMILAR TECHNOLOGIES

Our App and Website use cookies, SDKs, and similar tracking technologies to provide, analyze, and improve your experience. These technologies help us understand how you use Swimka, remember your preferences, prevent fraud, and deliver targeted advertisements. This section explains what these technologies are, how we use them, and how you can control their use. We are committed to transparency regarding tracking and are striving to implement additional consent management tools to give you granular control over which technologies collect your data.

6.1 Cookies & Web Tracking

Cookies are small data files stored on your device that help us provide and improve the Swimka experience. We use different types of cookies for different purposes, and we categorize them based on whether they are essential (required for the service to function) or optional (used to improve your experience and track usage):

Essential Cookies:

- laravel_session: Server-side session management required for authentication (expires at end of session)
- XSRF-TOKEN: CSRF protection via Laravel Sanctum, required for security (expires at end of session)
- locale: Stores your preferred language and regional settings (functional/essential)
- OAuth WebView session cookies: Secure cookies created during authentication with Strava, Garmin, Coros, Suunto, Polar, and Huawei (expires at end of session)

Website Cookies (swim-ka.com):

- Session and security cookies for form protection
- Google/Firebase Analytics (usage tracking)
- Meta Pixel (advertising retargeting)

For website cookies, we use both strictly necessary cookies (no consent required) and optional cookies (requiring consent; you can opt out via browser settings or cookie banners).

6.2 Mobile SDKs & In-App Tracking

Our App includes the following SDKs and libraries:

SDK	Provider	Purpose	Data Collected	Essential/Optional
Firebase Messaging	Google (US)	Push notifications	FCM device token, message interactions	Optional
Firebase Remote Config	Google (US)	Feature flags, app version checks	App version/build, config parameters	Essential

Facebook SDK	Meta (US)	Facebook login, auto app events	Facebook app ID, event data	Login: Essential; Auto events: Optional
Airbridge	Airbridge (US)	Mobile attribution, marketing analytics	Event data, install source	Optional: : consent in the EU and UK
Sentry	Sentry (US)	Crash/error monitoring	Error logs, stack traces and device context; personal details switched off	Essential
Google Sign-In	Google (US)	Google authentication	Google auth credentials	Essential (if user chooses)
Brevo	Brevo (France)	Email delivery, marketing automation	Email address, engagement tracking	Essential (transactional); Optional (marketing)
RevenueCat	RevenueCat (US)	In-app purchases and subscriptions	Purchase events, subscription status, user ID	Essential
Mixpanel	Mixpanel (EU data residency)	Product analytics	Usage events linked to your account number; no name, email, city, year of birth, pace, life-stage answers or chats	Optional: consent in the EU and UK
Mux	Mux (US)	Training video hosting and playback statistics	Playback events, device and network information, IP address	Essential (to play videos)
Apple Maps (MapKit)	Apple (US)	Looking up your city by name	The city name you type	Essential (if you add a city)

Opt-Out Mechanisms:

- Push notifications: Opt out in App Settings > Preferences > Notifications
- Third-party fitness integrations: Disconnect in App Settings > Connected Apps. This revokes access and removes stored OAuth cookies on our backend.
- Analytics and marketing consent management: We rely on your consent to utilize non-essential analytics and marketing SDKs where required by applicable law. If you are in the EU or UK, Mixpanel and Airbridge run only if you tap “Accept” on the “Help us improve Swimka” screen shown when you first open the App. You can change your choice at any time in My Account.

6.3 Global Privacy Control (GPC) & Do Not Track (DNT)

We do not currently respond to Global Privacy Control (GPC) or Do Not Track (DNT) signals in browsers or apps. However, you can control your privacy preferences directly through:

- App Settings (push notifications, connected accounts)
- Your web browser privacy settings

We are evaluating the technical implementation of GPC and DNT signal support and will update this section when available.

6.4 Third-Party Analytics & Social Media Pixels

- Meta / Facebook: We use Meta advertising tools to run retargeting ads outside the App. Meta may receive app usage events and conversion data; we do not send your advertising identifier. You can manage Meta ad preferences at facebook.com/adpreferences.
- Airbridge: Used for mobile app attribution — identifying how users discover and install Swimka. Collects install source and conversion events. If you are in the EU or UK, Airbridge runs only with your consent.
- Mixpanel: Used for product analytics, with data held in the EU. If you are in the EU or UK, Mixpanel runs only with your consent.

7. INTERNATIONAL DATA TRANSFERS

Swimka operates globally and engages service providers in multiple jurisdictions. This section explains how we manage the transfer of your personal information across international borders and what protections we have implemented to ensure your data remains protected even when transferred outside the European Union. We take

international data transfers very seriously and have implemented multiple legal mechanisms to ensure adequate protection.

7.1 Data Location & Transfer Mechanisms

General Principle:

We store and process data in the European Union and, when necessary, transfer data to the United States, and other countries for service delivery, analytics, and legal compliance. Any international transfers are conducted in strict accordance with applicable data protection laws and use approved transfer mechanisms. Our AI features run in the EU: Claude is accessed through AWS in EU regions only (Paris, Ireland, Frankfurt, Stockholm, Milan or Spain), Bubble's memory is stored by AWS in Paris, conversation transcripts are stored by DigitalOcean in Frankfurt, and Mixpanel holds analytics data in the EU. Some providers, such as Sentry, RevenueCat, Airbridge and Mux, may process data in the United States.

Specific Mechanisms:

For EEA/UK to US Transfers:

- Where a US provider is certified under the EU-US Data Privacy Framework (and its UK Extension), we rely on that certification
- Otherwise, we rely on Standard Contractual Clauses (SCCs) as approved by the European Commission under GDPR Article 46.2(c) and UK GDPR Article 46.2(a)
- For UK data: We use the UK International Data Transfer Agreement (UK IDTA) or UK addendum to SCCs as required by UK GDPR Schedule 1, Part 1
- We implement technical and organizational safeguards for international transfers, including data minimization, encryption (in transit and at rest), and access controls

For Other Non-Adequate Jurisdictions: We rely on appropriate safeguards, including binding corporate rules (if applicable), your explicit consent, and derogations for contract performance or legal necessity.

7.2 Risk of Transfers to the United States

Since July 2023, the European Commission has recognized US organizations certified under the EU-US Data Privacy Framework as providing adequate protection. For other US providers, we rely on Standard Contractual Clauses and additional safeguards. US authorities may in some cases seek access to data held in the United States.

7.3 Third-Party Integrations & Your Control

When you authorize third-party fitness app integrations (such as Garmin, Apple Health, COROS, Suunto or Strava), your data flows directly to those platforms according to their respective privacy policies and terms of service. You control these integrations and can disconnect at any time. We are not responsible for their data handling, but we maintain contractual arrangements where possible.

7.4 User Rights Regarding Transfers

If you are in the EEA/UK, you have the right to contact us with concerns regarding international transfers and request further information about the applicable safeguards, including a copy of them. Please contact us (contact@openswim.fr) to discuss alternatives or request a data transfer limitation.

8. HOW LONG WE KEEP YOUR INFORMATION

We retain personal information for as long as necessary to: provide the App and fulfill your requests, comply with legal, regulatory, or tax obligations, resolve disputes and enforce our agreements, and protect against fraud, security threats, and abuse. Data retention is carefully managed to balance your privacy interests with legitimate business needs and legal requirements. This approach ensures we do not retain your information longer than necessary while maintaining sufficient records to meet legal obligations and protect your interests and ours.

8.1 Retention Schedule

Active Account Data:

Retained while your account is active. Upon account closure, all personal information is deleted automatically, except where retention is required for legal, security, backup, dispute-resolution, or other disclosed purposes.

Inactive Accounts:

If you do not open the App for 24 months, we close your account and delete your personal information, keeping only anonymous totals. We email you a month before, so you can keep your account by opening the App, or download your swim history first. Accounts with an active paid Subscription are never treated as inactive.

For accounts that are already inactive for 24 months or more when this Policy takes effect, we will email you within three months of launch date and give you 30 days to sign in or download your swim history; if we don't hear from you, or the email bounces, we will delete the account.

Workout & Activity Data:

Retained indefinitely while your account is active. Upon account closure, we delete your swim history and keep only anonymous totals that cannot be linked back to you.

Third-Party Integration Data:

Data synced from connected fitness apps and devices is retained according to your third-party accounts' retention policies. You control syncing and can disable at any time.

Conversations with Bubble:

Transcripts are deleted automatically 30 days after the conversation ends. You can delete them sooner in My Account.

Bubble's Memory:

Cleared automatically 12 months after you last chat with Bubble, or sooner if you clear it in My Account (clearing her memory also deletes your conversations).

AI Processing by AWS:

AWS may keep prompts and replies for up to 30 days to detect abuse, and then deletes them. Our AI service's technical logs contain no conversation content and are kept for 30 days.

Life-Stage Answers:

Kept until you change or delete them in your profile. If you don't confirm them when we ask you to review them every six months, we delete them.

Permission Records:

Kept while your account is active and for five years after it is closed, so we can show which permissions you gave.

FFN License Number:

Kept until you remove it or your account is closed.

Support & Communication Data:

Customer support emails and correspondence are retained for up to 6 years after account closure for dispute resolution and service improvement, after which they are deleted or anonymized.

Technical & Analytics Data:

- Sentry crash logs and error reports: per Sentry's retention policy (typically 90 days)
- Airbridge attribution data: per Airbridge's retention policy
- Mixpanel analytics: when your account is deleted, we ask Mixpanel to delete your events and profile, which Mixpanel completes within a few weeks

Cookie Data:

- Session cookies (laravel_session, XSRF-TOKEN): deleted at end of session
- Locale cookie: persistent until manually cleared
- OAuth WebView cookies: related session tokens are revoked and associated server-side session data is cleared when you disconnect the integration

Backup & Archive Data:

DigitalOcean automatic database backups plus 30-day retention on QA server via custom backup script. Backup data is purged on a rolling basis.

8.2 Right to Deletion

You have the right to request deletion of your personal information, subject to legal exceptions. Please see Section 10 (Your Privacy Rights) for exercise instructions. Note that:

- Deletion of your account in App Settings will initiate automatic deletion of personal data
- Anonymized and aggregated data may be retained indefinitely
- Support emails are retained for legal and dispute resolution purposes
- Backup data may persist for up to 30 days after deletion from active systems
- Some data may be retained where required by law (tax, fraud prevention)

9. HOW WE PROTECT YOUR INFORMATION

We maintain reasonable and appropriate security measures to protect your personal information against unauthorized access, alteration, disclosure, and destruction. Security is a critical priority for Swimka, and we implement a multi-layered approach combining technical safeguards, organizational procedures, and vendor management practices to ensure your data remains confidential and secure throughout its lifecycle with us.

9.1 Technical Safeguards

- Encryption: Data is encrypted in transit (TLS/SSL) and at rest on our servers
- Secure Servers: Hosted by DigitalOcean (Frankfurt, Germany) and Amazon Web Services (EU) with industry-standard security
- Access Controls: Role-based access controls limit employee access to personal data on a need-to-know basis
- Bubble Conversations: Access is limited to the people who need it; conversation review uses pseudonyms, and every export is logged
- Authentication: Optional Face ID or Touch ID lock on the App
- API Security: Rate limiting, CORS protection, CSRF tokens (Laravel Sanctum XSRF-TOKEN)

9.2 Organizational Safeguards

- Security Policies: Data handling policies, incident response procedures
- Vendor Management: Contractual requirements for service providers
- Data Minimization: We limit collection and retention to what is necessary for stated purposes
- Confidentiality: All staff and vendors are bound by confidentiality obligations

9.3 Limitations & Incident Response

No Absolute Guarantee:

While we implement security best practices, no method of transmission over the Internet is 100% secure. We cannot guarantee absolute security, and you use the App at your own risk.

Breach Detection:

We monitor for breaches using Sentry (application errors and exceptions), server logs (Nginx/Apache for suspicious activity), and Laravel application logs.

Breach Notification:

If we experience a data breach that compromises your personal information, we will notify you and relevant authorities as required by GDPR (Art. 33-34), UK GDPR, French CNIL regulations, and applicable U.S. state breach notification laws within the required timeframe (typically 72 hours for GDPR).

10. YOUR PRIVACY RIGHTS

Your privacy rights depend on your jurisdiction. This section describes your rights under GDPR/UK GDPR (EEA/UK residents), U.S. state privacy laws (U.S. residents), and how to exercise them. Swimka is committed to honoring your privacy rights and providing you with meaningful control over your personal information. The rights outlined in this section are not mere suggestions but legal entitlements that we respect and enforce. We have implemented processes and systems to facilitate the exercise of these rights, and we handle all requests with diligence and care to ensure your rights are protected.

10.1 Privacy Rights for EEA/UK Residents

If you are located in the European Union, United Kingdom, or any jurisdiction subject to GDPR or similar laws, you have the following rights. These rights are fundamental to data protection law and reflect the principle that individuals should have meaningful control over their personal information. Swimka recognizes and respects

these rights fully, and we have implemented procedures to respond to requests promptly and fairly. Each right is described in detail below with specific instructions on how to exercise it.

A. Right of Access

You have the right to request access to the personal information we hold about you, including: what data we collect and why, who has access to your data, how long we retain it, and your rights regarding your data.

How to Exercise:

Send a written request to contact@openswim.fr with the subject line “Data Access Request”. We will provide your data in a structured, commonly used, and machine-readable format (CSV or JSON) within 30 days.

B. Right to Rectification

You have the right to request correction of inaccurate or incomplete personal information.

How to Exercise:

Update your profile information directly in App Settings. For data we cannot correct within the App, submit a request to contact@openswim.fr with the subject line “Data Correction Request”. We will correct information within 30 days.

C. Right to Erasure / “Right to Be Forgotten”

You have the right to request deletion of your personal information, subject to legal exceptions (tax/accounting obligations, legal claims, fraud prevention).

How to Exercise:

Submit a written request to contact@openswim.fr with the subject line “Data Deletion Request”. Include details of what data you wish deleted. We will delete information within 30 days, unless we must retain it due to legal obligations or legitimate purposes. Note: Deletion of your account in App Settings will initiate an account closure process. Personal data will be deleted automatically, except as required by law.

D. Right to Restrict Processing

You have the right to request that we limit processing of your data (e.g., suspend marketing, analytics) while you dispute accuracy or lodge a complaint.

How to Exercise:

Submit a written request to contact@openswim.fr with the subject line “Data Processing Restriction Request”. Specify the restriction you seek. We will honor restrictions within 30 days, except where processing is necessary for service delivery or legal compliance.

E. Right to Data Portability

You have the right to receive a copy of your personal information in a structured, commonly used, machine-readable format and to transmit it to another controller.

How to Exercise:

Submit a request to contact@openswim.fr with the subject line “Data Portability Request”. We will provide an export (CSV, JSON) of your account data, workout records, and profile information within 30 days. We will also facilitate direct transfer to another service upon request, where technically feasible and legally required.

F. Right to Object

You have the right to object to processing of your personal information on grounds of legitimate interests, including for direct marketing.

How to Exercise:

- For Marketing: Opt out via email preferences in your account settings, or click “Unsubscribe” in marketing emails, or contact contact@openswim.fr
- For Other Processing: Submit a written objection to contact@openswim.fr with the subject line “Objection to Processing”, specifying the processing you object to and your reasons. We will cease processing within 30 days unless we demonstrate compelling legitimate interests or legal obligations.

G. Right to Human Review of Automated Decision-Making

If we make a decision based solely on automated processing that produces legal or similarly significant effects, you have the right to: obtain human review by a company representative, express your views on the decision, and request manual reconsideration.

How to Exercise:

Contact contact@openswim.fr with the subject line “Request for Human Review”. Specify the automated decision. Note: our AI features make suggestions only and do not make decisions with legal or similarly significant effects (see Section 12), but you can still ask a person to review an AI suggestion.

H. Right to Lodge a Complaint with a Supervisory Authority

If you believe we have violated your data protection rights, you may lodge a complaint with your national data protection authority:

- France (CNIL): Commission Nationale de l'Informatique et des Libertés. Website: www.cnil.fr. Email: plaintes@cnil.fr. Postal: CNIL, 3 Place de Fontenoy, 75007 Paris, France.
- United Kingdom (ICO): Information Commissioner's Office. Website: www.ico.org.uk. Email: icocasework@ico.org.uk. Postal: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK.
- Other EU Member States: See https://edpb.europa.eu/about-edpb/about-edpb/members_en for links to national authorities.

I. Post-Mortem Data Rights (French Law)

Under French law, your heirs may, after your death, contact us to: request access to certain accounts and messages for archival or memorial purposes, and request deletion of your account.

How to Exercise:

Submit a request with proof of authorization (death certificate, executor documentation) to contact@openswim.fr.

J. Right to Withdraw Consent

Where processing is based on your consent (for example Bubble, the life-stage questions, conversation review, analytics and attribution, sharing with a Club partner, push notifications, precise geolocation and marketing emails), you may withdraw consent at any time via My Account or Settings in the App, by clicking “Unsubscribe” in marketing emails, or by contacting contact@openswim.fr. Withdrawal does not affect the lawfulness of processing before withdrawal.

10.2 Privacy Rights for U.S. State Residents

If you are a resident of California, Colorado, Connecticut, Utah, Virginia, Texas, or another U.S. state with applicable privacy laws, you may have certain rights regarding your personal information under those laws, depending on how those laws apply to Swimka and your relationship with us. These rights may include, for example, rights to access, delete, correct, or limit certain uses of your personal information, subject to applicable exceptions and limitations. Swimka is committed to respecting privacy rights and, where applicable, facilitating requests in accordance with relevant U.S. state privacy laws.

A. Right to Know (Access)

You may have the right to request what personal information we collect, use, disclose, and retain about you over the preceding 12 months.

Categories of PI Collected:

Identifiers, internet activity, geolocation, health information, inferences (such as AI-generated training plans and coaching suggestions), sensitive personal information (health information you choose to give us), commercial information (purchases/subscriptions).

Sources:

Directly from you (registration, profile), automatically from device (analytics, cookies, SDKs), from third parties (fitness apps, service providers).

Purposes:

Contract performance, analytics, personalization, fraud prevention, legal compliance, marketing.

Categories Disclosed/Shared:

Service providers, third-party fitness apps, law enforcement (upon legal process), aggregated/de-identified data.

How to Exercise:

Submit a request to contact@openswim.fr with the subject line “Right to Know Request”. Provide sufficient information to verify your identity (name, email, account ID). We will provide your personal information within 45 days in a portable, machine-readable format.

B. Right to Delete

You may have the right to request deletion of personal information we have collected from you, subject to limited exceptions (legal obligations, fraud prevention, service delivery obligations).

How to Exercise:

Submit a request to contact@openswim.fr with the subject line “Right to Delete Request”. We will delete your information within 45 days, except: information retained for legal/tax obligations, information necessary to complete transactions you initiated, information retained for fraud, abuse, or security prevention, and aggregated or de-identified data (not linked to you).

C. Right to Correct

You may have the right to request correction of inaccurate personal information we maintain about you.

How to Exercise:

Update your profile in App Settings, or submit a request to contact@openswim.fr with the subject line “Right to Correct Request”. We will correct information within 45 days.

D. Right to Opt-Out of Sale & Sharing

You may have the right to direct us not to sell or share your personal information. While we do not sell personal information for monetary compensation, we engage in "sharing" (as defined under applicable laws) of personal information with third-party advertising partners for the purpose of cross-context behavioral advertising and performance attribution.

How to Exercise:

Submit an opt-out request to contact@openswim.fr with the subject line “Opt-Out Request”. We will process and confirm the opt-out request within 15 days.

E. Right to Limit Use of Sensitive Personal Information (CPRA)

If we collect sensitive personal information (health data, precise geolocation), You may have the right to limit our use of such information to what is necessary to provide the services you request.

Categories of Sensitive PI Collected:

Health information (life-stage answers and health information you share with Bubble) and precise geolocation (routes of open-water swims recorded by a watch).

How to Exercise:

Submit a request to contact@openswim.fr with the subject line “Limit Sensitive PI Request”. Specify which sensitive PI uses you wish to limit. We will comply within 45 days and will use sensitive PI only for disclosed service purposes.

F. Right to Non-Discrimination

We will not discriminate against you for exercising your privacy rights. Specifically, we will not: deny goods or services, charge different prices or rates, provide different quality of service, or retaliate or penalize you.

G. Authorized Agent (Minors & Power of Attorney)

If you are a minor (under 18 in some states, under 13 in others), or if you appoint an authorized agent, they may submit privacy requests on your behalf. Authorized agents must provide proof of authority (legal documentation, power of attorney), provide their own identity verification, and submit requests in writing to contact@openswim.fr with the subject line “Privacy Request.” We will verify the agent's authority before processing the request.

H. Appeal Process

If we deny your privacy request, You may have the right to appeal our decision.

How to Appeal:

1. Submit a written appeal to contact@openswim.fr with the subject line “Privacy Request Appeal”. 2. Specify the original request, our denial reason, and why you believe the denial was incorrect. 3. We will review your appeal and issue a final decision within 45 days. 4. You may also contact your state attorney general or file a complaint with your state's privacy authority.

10.3 How to Exercise Your Rights

Submission Methods:

- Email: contact@openswim.fr (subject line should specify request type: “Data Access,” “Data Deletion,” “Data Correction,” “Limit Sensitive PI,” “Appeal,” etc.)
- In-App: Account Settings > Privacy (when available)
- Postal Mail: SSO Active, 12 rue Fernand Léger, 91440 Bures-sur-Yvette, France (marked “Privacy Request”)

Verification of Identity:

To protect your privacy and security, we will verify your identity before processing privacy requests. We may ask for: your account email and username, last four digits of payment method (if applicable), and other information tied to your account.

Response Timelines:

- EEA/UK: We aim to respond within 30 days of receipt. Complex requests may be extended by 60 days with notice.
- U.S. States: We aim to respond within 45 days of receipt.

We will notify you in writing (email or in-app) of our decision, including any denial reasons and appeal options.

Assistive Technology:

If you have accessibility needs, please inform us in your request, and we will provide your data in an accessible format.

Nothing in this section 10 is intended to state that any particular U.S. state privacy law currently applies to Swimka in all circumstances; rather, Swimka provides this notice to describe rights that may be available where applicable.

11. CHILDREN'S PRIVACY

SWIMKA IS INTENDED FOR USERS AGED 18 AND OLDER ONLY. We do not knowingly collect personal information from individuals under 18 years of age, in compliance with our Terms of Service and applicable law (including COPPA in the United States). Protecting children's privacy is a fundamental principle that guides our operations. We take a proactive approach to preventing unauthorized access to our platform by minors and implement multiple safeguards to ensure compliance with applicable child protection laws in all jurisdictions where we operate.

Age Confirmation:

We ask every user to confirm that they are 18 or over at sign-up (and existing users when they first open the updated App), and record the confirmation and its date.

If a year of birth added later shows that a user is under 18, we close the account.

What We Do:

- No Knowing Collection: We do not solicit or intentionally collect information from anyone under 18. Our Terms of Service (Section 2.2) require users to confirm they are 18 or older.
- Parental Safeguards: If a parent or guardian becomes aware that a person under 18 has created an Swimka account, they should contact us immediately at contact@openswim.fr for account deletion.

If We Discover a Minor User:

If we discover that a minor has created an account: 1. We will immediately suspend or delete the account. 2. We will delete all associated personal information within 30 days, subject to legal obligations. 3. We will attempt to notify the account holder or parent/guardian.

U.S. COPPA Compliance:

Swimka does not knowingly collect, use, or disclose personal information from children under 13 years of age in the U.S., in compliance with the Children's Online Privacy Protection Act (COPPA). If we discover a child under 13 has provided personal information, we will delete it and notify the child's parent/guardian.

Questions About Child Privacy:

If you are a parent or guardian concerned about your child's data privacy on Swimka, please contact us at contact@openswim.fr with details, and we will address your concerns promptly.

12. AI FEATURES: BUBBLE, AI TRAINING PLANS AND THE DAILY COMMENT

12.1 What the AI Features Are

Swimka uses AI in three features (the "AI features"): AI training plans, which build and update your plan; the daily comment on your home screen; and Bubble, an AI swim coach you can chat with. They run on Claude, an AI model made by Anthropic, which we access through Amazon Web Services (AWS) using its Bedrock service, in EU data centers only. AWS does not use your information to train AI models and does not share it with Anthropic. The App tells you that Bubble is an AI at the start of each chat.

12.2 What Each Feature Uses

- **AI training plans**: your profile (such as your level, goals, strokes, pool or open water, reasons for swimming and sessions per week), your plan and your recent swims.
- **Daily comment**: your first name, the training details in your profile (such as level, pace, strokes, goals and reasons for swimming), a summary of your plan, your last five swims (date, distance, duration, stroke, place and pace), this week's totals and your consistency over four weeks. It never uses heart rate, anything you type, Bubble's memory, your age, gender, city, weight or height, or your life-stage answers.
- **Bubble**: your profile, your plan and your swims, your conversations with her, her memory of you, and your life-stage answers if you have given them. If you tell her about an injury, your health or your life stage, she uses it to adapt your training.

12.3 Your Permissions

- Before your information is first sent to Claude, we ask your permission in the App: when you create your first AI training plan (this also turns on the daily comment) and when you first open Bubble. If you already use Swimka, we ask before your information next goes to Claude. Until you agree, your home screen shows text we have written ourselves, and ready-made plans are available.
- Bubble's permission screen also asks for your explicit consent to use any health information you share with her.
- We provide AI training plans and the daily comment to perform our contract with you. For Bubble, we rely on our contract with you and, for health information, on your explicit consent.
- You can switch Bubble off at any time in My Account; after that, nothing more from your chats is sent to Claude. To withdraw your permission for AI training plans and the daily comment, contact us at contact@openswim.fr.

12.4 Memory, Conversations and Review

- Bubble keeps notes about you between chats, so you don't have to repeat yourself. You can read them and clear her memory in My Account; clearing her memory also deletes your conversations. Her memory is cleared automatically 12 months after you last chat with her.
- Conversation transcripts are stored in the EU and deleted automatically 30 days after the conversation ends.
- If you report a problem with Bubble, we may look at the conversation concerned to help you.
- **Conversation review (optional):** with your separate consent, given by a box on Bubble's permission screen, our team may read your conversations under a pseudonym, never your name or email, to see where Bubble can do better. You can remove permissions at any time in My Account.
- We also use content-free figures, such as the number and length of conversations and what they cost, to run and improve the service. Our AI service's technical logs contain no conversation content and are kept for 30 days.

12.5 Coaching, Not Medical Advice, and No Automated Decisions

- **Bubble is a training coach, not a doctor.** She adapts your training around an injury or life stage and suggests seeing a doctor or other professional about the condition itself. The AI features can make mistakes, so check anything important.
- **The AI features make suggestions only.** They do not make decisions that have legal or similarly significant effects on you, such as closing your account or refusing you a service, so Article 22 GDPR does not apply. You can ignore any suggestion, change your goals or preferences, switch Bubble off, or ask a person to review an AI suggestion by emailing contact@openswim.fr with the subject line "Request Human Review".

13. THIRD-PARTY LINKS AND SERVICES

The Swimka App and Website may contain links to external websites and services (fitness tracking platforms, social media, external trainers, event organizers, etc.). This Privacy Policy covers only Swimka and does not apply to third-party services. While we carefully select our integration partners and conduct due diligence on their privacy practices, we cannot control how third parties handle your personal information once it leaves our platform. We encourage you to review their privacy policies independently and exercise caution when sharing information with external services.

Your Responsibilities:

- Review Third-Party Policies: We encourage you to review the privacy policies of any third-party services before linking your accounts or providing information
- No Control Over Third Parties: We do not control third-party privacy practices and are not responsible for their data handling
- Integrations: When you authorize Swimka to integrate with a fitness app or device (such as Garmin, Apple Health, COROS, Suunto or Strava), your data is governed by those platforms' privacy policies

Third-Party Fitness Integrations:

Swimka explicitly supports integrations with: Garmin Connect, Apple Health & Apple Watch, COROS, Suunto and Strava. The list in the App is always up to date.

When you authorize these integrations, you grant Swimka permission to: receive your fitness data from the third-party platform (via API), share your Swimka workout data with the third-party platform, and sync and display third-party data within Swimka.

You control integrations entirely: You can connect or disconnect integrations at any time in your App Settings. Disconnecting an integration will stop data syncing; previously synced data may remain in Swimka (you can request deletion separately).

Clubs and Partner Sites:

Club pages may link to a partner's shop or to an event registration site run by a partner or another platform. What you do there is governed by that site's privacy policy.

Embedded Content:

The App and Website may embed content (videos, images, promotional material) from third parties. For example, some older training videos are played through YouTube. Such embedded content may include tracking pixels, cookies, or scripts. We do not control third-party tracking; review their privacy policies as needed.

14. 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 other factors. Our commitment to transparency extends to how we communicate changes to this Privacy Policy. We understand that you need to understand how our practices may evolve, and we are committed to providing you with clear notice and, where required by law, obtaining your consent before material changes take effect. We will notify you of material changes by:

- Email Notification: Sending an email to your registered account address (if significant changes)
- In-App Notification: Displaying a prominent notification within the App
- Website/App Notice: Posting the updated policy on the App and Website with a clear "Last Updated" date
- User Consent (if required): Requesting your affirmative consent to material changes before your continued use of the App

Effective Date:

The effective date of this Privacy Policy is listed at the top. If we make changes, we will update this date.

Your Rights Upon Changes:

If you do not agree with material changes, you may discontinue your use of Swimka and delete your account. Where a change affects something you consented to, we will ask for your consent again.

15. CONTACT US

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us using the methods provided below. We value your feedback and inquiries regarding privacy matters and are committed to responding promptly and thoroughly. Whether you have a question about how we handle your data, wish to exercise a privacy right, or want to report a concern, our team is ready to assist you. We have implemented procedures to ensure your inquiries are handled professionally and confidentially.

SSO Active (Swimka)

Email:

contact@openswim.fr

Postal Address:

12 rue Fernand Léger, 91440 Bures-sur-Yvette, France

Response Timelines:

- We will acknowledge your request within 5 business days
- We will provide a substantive response within 30 days (EEA/UK) or 45 days (U.S. states), or notify you of reasonable extensions

Data Protection Officer:

SSO Active has determined that the appointment of a Data Protection Officer is not required under Article 37 GDPR at this time. For all privacy inquiries, please contact us at contact@openswim.fr.

END OF PRIVACY POLICY