BDYCTRL Privacy Policy

Piik Labs AB · Version 1.1.9

Effective date: 20 November 2026 **Last updated:** 20 November 2026 **Applies to:** the BDYCTRL mobile application (iOS), the BDYCTRL app on Apple Watch, and the website at bdyctrl.com

1. Who we are

This Privacy Policy applies to **Piik Labs AB**, a company registered in Sweden with organisation number 559577-8506 (the "Company", "we", "us", "our").

We operate the BDYCTRL mobile application (the "App") and the website at bdyctrl.com (together, the "Services").

As the entity that determines the purposes and means of processing your personal data, Piik Labs AB acts as the **data controller** under the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and the Swedish Data Protection Act (lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).

1.1 Scope: which product this policy covers

> **BDYCTRL is a Piik Labs brand.** Piik Labs AB operates other products and services under separate brands. This Privacy Policy applies only to the BDYCTRL App and the bdyctrl.com website. Other Piik Labs products are governed by their own separate privacy policies, and the processing described here does not extend to them.

1.2 Contact

Data controller	Piik Labs AB
Organisation number	559577-8506
VAT number	SE559577850601
Registered address	Box 691, 414 52 Göteborg, Sweden
Privacy enquiries	privacy@bdyctrl.com
Legal and compliance	legal@bdyctrl.com
Supervisory authority	Integritetsskyddsmyndigheten (IMY), imy.se · imy@imy.se

Data Protection Officer. We have not designated a Data Protection Officer under Article 37 GDPR, as we are not required to do so. All privacy matters are handled directly by the Company and should be directed to privacy@bdyctrl.com.

2. Scope of this policy

This Policy applies to all personal data we collect when you use the Website or the App, create an account, contact us, or take part in a survey, beta programme, or promotion. It does not apply to third-party websites or services linked from the Services.

3. Personal data we collect

We collect personal data in three ways: data you actively provide, data generated automatically through your use of the Services, and data we receive from third parties. We also generate derived data about you, described in section 3.4.

3.1 Data you provide

Account and identity data

- Full name
- Display name (the name you choose to go by in the App)
- Email address
- Password (stored in hashed form; we never store plain-text passwords)
- Profile photo and cover photo (optional)
- Date of birth (used to confirm you meet the minimum age for the Services and to apply the protections for users under 18, see sections 3.5 and 11)
- Gender (optional)
- Profile ID: a random number assigned to your account, which you can share with people you want to connect with and replace at any time
- Interests you add to your profile (optional)

Health and fitness data

- Body weight, height, and BMI
- Body measurements (e.g. waist, chest, arms, legs)
- Workout logs: exercises, sets, reps, weights, duration
- Activities you record, such as runs, walks and hikes: distance, duration, pace and elevation
- Photos you take while recording an activity and add to it (optional)
- Training programmes selected or created by you (BDYSessions, BDYBlocks, BDYCycles)
- Progress photos, if you choose to upload them
- Muscle recovery status and fatigue indicators
- Subjective wellbeing or energy levels, if entered

AI coaching and plan data

- Fitness goals, experience level, and preferences you provide during onboarding
- Messages you send to Bolt, our AI coaching feature
- Inputs used to generate personalised AI workout plans
- AI-generated plan outputs stored to your profile

Nutrition data (future feature)

- Food logs, macro and calorie tracking data
- Dietary preferences or restrictions

Payment data

- Subscription status, entitlement level, and purchase history

- Apple App Store purchase receipts
- Refund requests and subscription changes

All payments are processed by Apple. We do not collect, receive, or store your payment card details at any point. See section 6.1 for the providers involved.

Communications data

- Messages sent to our support team
- Survey responses and feedback
- Any other content you voluntarily submit to us

3.2 Data collected automatically

Usage and technical data

- Device type, operating system, and app version
- Unique device identifiers
- IP address
- Screen views, feature interactions, and navigation patterns
- Session duration and frequency of use

Service logs. Our backend platform records each request the App makes to our servers, including the request headers, which contain your IP address. These logs exist so that we can diagnose faults and investigate misuse. They are held for 24 hours on a rolling basis and are then deleted automatically.

Website visits. When you visit bdyctrl.com, we collect visit statistics as described in section 10.

Diagnostic and crash data

When the App encounters an error or crashes, we collect diagnostic information to identify and fix the fault. This includes the device model, operating system version, app version, the sequence of screens and actions leading up to the error, and technical error details. This data is processed by Sentry (see section 6.1).

Each report carries your BDYCTRL account identifier (an internal number, not your email address), so we can see how many people a fault affects. It is removed when you sign out. We do not send your email address, authentication tokens, IP address, or any health or measurement data.

Product analytics

If you agree to product analytics during account setup, we record how you use account setup, the subscription offer and your first steps in the App, such as the screens you open, the buttons you tap, your subscription choice and the time each step takes. Events carry a random identifier stored on your device and, once you have an account, your BDYCTRL account identifier, together with your device type, operating system, app version and country. Country is derived from your IP address, which is then discarded. You can withdraw this consent at any time in Settings. This data is processed by PostHog (see section 6.1).

Location data

City and country. With your permission, the App checks your device's location at two points: when you set up your account, and when you complete a workout. The coordinates are resolved to a city and country name on your device, and only that label is sent to us. The label from signup sets your profile

location; the label from a workout is stored with that workout's record and is used to show you your own activity history.

You grant this permission on your device and can withdraw it at any time in your device settings. You can also turn location use off in the App under Settings, which clears the city and country we hold and stops new labels being recorded. The device permission stays as you set it until you change it there.

Recorded activities. When you record an activity, such as a run, walk or hike, the App processes your device's precise location from start to stop, including while the screen is locked or the App is in the background. It uses the location to measure the activity and record its route. If you record on Apple Watch, the Watch processes it instead (see section 13). With your consent to save routes, we store the route with the activity. Without that consent, we store the activity without its route, and the route stays on your device. Your full route is visible only to you. Where other users can see an activity, they see a separate copy of the route with its start and end hidden (see section 3.5). How long routes are kept is set out in section 8.

Activity photos. We store the photos you add to an activity. Before a photo is stored, we remove the location and camera data saved in the image file. With your consent to save routes, we store the point on your route where the photo was taken. Activity photos and their locations are visible only to you. If you use a photo in something you share, we store a separate copy of it for that, without a location.

Withdrawing. You can withdraw your consent to save routes at any time in Settings. We then delete the routes we store and the locations of your activity photos. Your activities and photos stay, without their locations.

Community. Your city and country are also used to show you people and challenges in the same city or country, and they can be visible to other users as described in section 3.5.

Time zone

Read from your device's regional settings, not from your location. Used to schedule notifications, weekly reports, and usage resets at times that make sense where you are. Your time zone is sent whether or not you grant the location permission.

Language

Read from your device's language setting. Used to reply to you in your language, including when Bolt answers you.

Push notification token

If you grant notification permission, your device is issued a push notification token, a unique identifier that allows notifications to be delivered to your device. We store this token so that we can send you notifications, and we delete it when you revoke permission or delete your account. See section 6.1 for the providers involved in delivering notifications.

3.3 Data from third parties

- **Sign in with Apple**: name and email address (or Apple's private relay address) if you choose to authenticate this way. You can also register with an email address and password, or with a one-time code sent to your email.
- **Apple App Store**: purchase validation and subscription status data
- **Apple Health**: if you connect it, the data described in section 13.

3.4 Derived and generated data

In addition to data you provide and data we collect automatically, we generate new data about you by processing and analysing your inputs. This derived data is personal data and is treated with the same protections as the data it is derived from.

- **BDYCharge points and gamification metrics**: accumulated points, points per session, consistency metrics, and leaderboard position.
- **AI-generated insights and plans**: workout plans, performance trend analysis, recovery suggestions, and difficulty adjustments produced by Bolt and our AI plan generation.

This processing involves automated analysis of your personal data, including health and fitness data (special category data under GDPR Article 9). It is carried out on the basis of your explicit consent together with our contract with you. The AI does not make decisions producing legal or similarly significant effects. All outputs are recommendations that you choose whether to follow. You may request human review of any AI-generated output by contacting privacy@bdyctrl.com.

> **Bolt is an artificial intelligence system, not a human coach.** You are told this at the point of interaction within the App. AI-generated content is produced automatically and is not individually reviewed by a person, a medical professional, or a qualified trainer before it reaches you.

3.5 Community and shared content

When you use community features, we store your community profile, the content you share and the metadata attached to it, such as timestamps and interaction counts. This includes posts, comments, reactions, progress photos and workout summaries you share, who you follow and who follows you, follow requests, the users you block, reports you make, your participation in challenges, and your leaderboard positions.

Who can see it. Your community profile and what you share are visible to other signed-in BDYCTRL users, within the choices you make below. A profile can show your display name, profile and cover photos, city and country, interests, BDYCharge level, leaderboard positions and follower counts. A shared workout summary can show the exercises, sets, total volume, duration and performance score of that workout, and the city where it took place.

Your choices. Before anything of yours is shared, you choose whether your profile is public, whether your completed workouts are shared with the community, and whether you appear under your display name or under an anonymised identity. You can change each choice at any time in the App's settings. Workout data can be health data under GDPR Article 9, so sharing your workouts is based on your explicit consent, which you can withdraw at any time. A public profile can be found by other users by name and by city or country. A profile that is not public can only be found through its Profile ID.

Activities and routes. You choose who can see each activity you record. Other users who can see an activity can see its route, with its start and end hidden, and its distance, duration, elevation and approximate start time. You can hide the route, the pace and the start time of each activity.

Anonymised identity. An anonymised identity replaces your display name and photos with a generic name and shows your country instead of your city. Other users can see what is shared under it, but not who you are.

Profile ID. Your Profile ID reaches other people only when you give it to them. You can replace it at any time, and the old ID then stops finding you.

Users under 18. If you are 16 or 17, your profile is not public and cannot be made public until you turn 18. You do not appear in search or in suggestions of people near you. Your workouts are shared only if you choose to share them, and always under an anonymised identity. Content you post is visible only to followers you have approved, and anyone who wants to follow you needs your approval. The activities you record are visible only to you, and your routes are not shared. When you turn 18, your settings stay as they are until you change them.

Removing what you share. You can delete anything you post at any time, whatever your age. Deleting it removes it from the Services, but it does not guarantee complete removal: other users may already have copied it, and it can remain in backups for a limited period before they are overwritten. Where other users have interacted with your content, traces of that interaction may remain on their accounts.

Blocking and reporting. When you block someone, we store the block so that it can take effect. When you report content or a user, we store the report and the reported content so that we can review it.

We do not sell your content or your social connections, and we do not licence them to third parties. The one exception is a shared path, where the Services let you share one, which we may show in marketing for BDYCTRL, including advertising on other platforms, without anything that identifies you, as set out in section 10.5 of our Terms.

4. How and why we use your data

We only process your personal data where we have a valid legal basis under the GDPR. The table below sets out our processing purposes, the data involved, and the legal basis for each.

Purpose	Data used	Legal basis (GDPR)
Create and manage your account	Account and identity data	Art. 6(1)(b): contract
Confirm you meet the minimum age and apply protections for users under 18	Date of birth	Art. 6(1)(c): legal obligation Art. 6(1)(f): legitimate interest
Provide fitness tracking and analytics	Fitness, workout and body metric data	Art. 6(1)(b): contract Art. 9(2)(a): explicit consent
Provide AI coaching and generate workout plans (Bolt)	Goals, preferences, fitness and health data, summaries of your activities, chat messages	Art. 6(1)(b): contract Art. 9(2)(a): explicit consent
Set your profile location and record where a workout took place	City and country, derived on-device from a location check at signup and when you complete a workout	Art. 6(1)(a): consent (device permission)
Record your activities, and let you view and share them	Precise location while you record, activity summaries	Art. 6(1)(b): contract Art. 9(2)(a): explicit consent
Keep the routes of your activities	Routes	Art. 6(1)(a): consent (Save my routes)
Add photos to your activities and place them on your map	Activity photos, the point on your route where each was taken	Art. 6(1)(b): contract Art. 6(1)(a): consent (Save my routes, for the point on the route)
Show heart rate, energy and cadence on your activities, add workouts from Apple Health to	The Apple Health data listed in section 13	Art. 6(1)(a): consent (Apple Health) Art. 9(2)(a): explicit consent

Purpose	Data used	Legal basis (GDPR)
your history, and save the activities you record to Apple Health		
Show maps	IP address, device and operating system information, map areas requested	Art. 6(1)(b): contract
Reply to you in your language	Device language setting	Art. 6(1)(b): contract
Schedule notifications and reports in your local time	Device time zone	Art. 6(1)(b): contract
Generate BDYCharge points and rankings	Workout duration, session logs, derived points data	Art. 6(1)(b): contract Art. 6(1)(f): legitimate interest
Operate community features: profiles, following, the feed, shared activities, leaderboards and challenges	Community profile data, interests, content you share, shared workout summaries, shared activities and routes, social graph, interaction data	Art. 6(1)(a): consent (your visibility and sharing choices) Art. 9(2)(a): explicit consent (shared workout data)
Let people you choose find and connect with you	Profile ID, display name	Art. 6(1)(b): contract
Review reports and keep the community safe	Reports, blocks, reported content, account data	Art. 6(1)(f): legitimate interest
Process payments and manage subscriptions	Subscription and entitlement data	Art. 6(1)(b): contract
Send service and transactional notifications	Email address, push notification token	Art. 6(1)(b): contract
Send marketing communications and promotional push notifications	Email address, push token, preferences	Art. 6(1)(a): consent
Diagnose crashes and fix faults	Diagnostic and technical data, account identifier	Art. 6(1)(f): legitimate interest
Improve and develop the Services	Anonymised usage data, website visit statistics	Art. 6(1)(f): legitimate interest
Understand how new users set up their account and respond to the subscription offer	In-app events, account or device identifier, device and app version, country	Art. 6(1)(a): consent
Keep a record of the consents you give	Consent choices, policy version, time	Art. 6(1)(c): legal obligation
Ensure security and prevent fraud	Technical, account and usage data	Art. 6(1)(f): legitimate interest
Comply with legal obligations	Relevant data as required	Art. 6(1)(c): legal obligation
Respond to support requests	Communications and account data	Art. 6(1)(b): contract

> **Marketing push notifications are separate from service notifications.** Granting notification permission at the device level allows us to deliver notifications; it is not on its own consent to receive marketing. Promotional and re-engagement notifications are sent only if you separately opt in within the App, and you can withdraw that at any time in your notification settings without affecting service notifications.

5. Special category data and consent

Certain fitness and health data you provide (including body measurements, body weight, BMI, workout performance, recovery indicators, progress photos, and any health information you share with Bolt) may qualify as special category data under GDPR Article 9.

We process this data, including by our AI features, only with your explicit, informed consent. We ask for it when you set up your account, or once when you next open the App if your account is older. This consent is required to use the App. You can withdraw it at any time by deleting your account in Settings, after which your personal data is deleted as described in section 8. Withdrawal of consent does not affect the lawfulness of processing that occurred before withdrawal.

Sharing your workout data with other users is covered by a separate explicit consent, which you give or withhold when you make your community choices (see section 3.5). Withdrawing it stops new workouts being shared and does not affect the rest of the Services.

Apple Health data and the saving of your routes are each covered by their own explicit consent. Both are optional. We ask for each before it is first used, and you can withdraw either at any time in Settings without affecting the rest of the Services. See sections 3.2 and 13.

6. Third-party services and data sharing

We do not sell your personal data. We share data only with service providers who process it on our behalf under data processing agreements, and where required by law.

6.1 Service providers (data processors)

Infrastructure, backend and storage

- **Xano Inc. (USA)**: backend database and API hosting, and storage of publicly visible images such as profile photos and images you share to the community feed. All data is stored in the EU (Frankfurt, Germany, AWS eu-central-1 region). Data processing agreement in place.
- **Vercel Inc. (USA)**: hosting of the bdyctrl.com website, and private storage of progress photos and activity photos you upload from the App. These photos are held in private storage that is not publicly accessible and is retrievable only through an authenticated request from your own account. This data is stored in the EU region. Data processing agreement in place.

Maps

- **Mapbox, Inc. (USA)**: maps in the App. Receives your IP address, your device and operating system information, and the map areas requested. Mapbox processes this data under its data processing agreement. Review: mapbox.com/legal/privacy and mapbox.com/legal/dpa

AI processing

- **Anthropic PBC (USA)**: provider of the Claude family of large language models, accessed via the Anthropic API and used to power Bolt and AI-generated workout plans. Inputs sent to Anthropic

include your stated fitness goals, experience level, training preferences, relevant workout history, and the content of your messages to Bolt. Anthropic processes this data as our processor under a data processing agreement incorporating the European Commission's Standard Contractual Clauses. Your data is not used to train Anthropic's models. Bolt does not receive your routes, the locations of your activity photos, or the heart rate, active energy and steps the App reads from Apple Health. Review: anthropic.com/legal/privacy

Payments and subscriptions

- **Apple Inc. / Apple Distribution International Ltd. (Ireland)**: all payment transactions are processed within Apple's payment infrastructure. Apple is the merchant of record for App Store purchases in the EEA. We receive only confirmation of purchase status.
- **RevenueCat, Inc. (USA)**: subscription and entitlement management. Receives purchase receipt data from the App Store to determine your subscription tier and feature entitlements. No payment card data is processed by RevenueCat or by us. Where you install the App from an Apple Search Ads advert, RevenueCat also receives the related campaign and keyword from Apple. Review: revenuecat.com/privacy

Diagnostics and crash reporting

- **Functional Software, Inc. d/b/a Sentry (USA)**: application error monitoring and crash reporting. Our Sentry organisation is hosted in Sentry's EU region (Frankfurt, Germany), so diagnostic data is stored within the EU. We have disabled the transmission of personally identifying information by default; the only identifier we attach is your BDYCTRL account identifier. Data processing agreement in place. Review: sentry.io/privacy

Notifications

- **Apple Inc. (USA): Apple Push Notification service (APNs)**, the infrastructure that delivers notifications to your device. Apple issues the push token and routes the notification.
- **Exponent, Inc. d/b/a Expo (USA)**: push notification delivery service. Receives your push token and the content of notifications in order to deliver them to your device. Review: expo.dev/privacy

Analytics

- **PostHog, Inc. (USA)**: product analytics, for users who consent to it. All data is stored in the EU (Frankfurt, Germany). Data processing agreement in place. Review: posthog.com/privacy
- **Vercel Inc. (USA)**: website analytics for bdyctrl.com. Data may be processed in the United States. Data processing agreement in place. Review: vercel.com/legal/privacy-notice

We also receive aggregate, non-identifying usage statistics from Apple through App Store Connect, which you can opt out of in your device settings under Privacy & Security → Analytics & Improvements.

Email and communications

- **Postmark (Wildbit LLC, USA)**: transactional email delivery (account verification, password resets, purchase receipts, and security notifications). Review: postmarkapp.com/privacy-policy
- **Loops, Inc. (USA)**: marketing and engagement email (product updates, feature announcements, and community communications). Only sent to users who have opted in. Review: loops.so/privacy
- **Microsoft Ireland Operations Limited** (Ireland): Microsoft 365, which hosts the mailboxes behind privacy@bdyctrl.com and legal@bdyctrl.com and therefore stores your message and our reply if you write to us. Microsoft processes this data as our processor under the Microsoft Products and Services Data Protection Addendum. Under Microsoft's EU Data Boundary, customer data for Microsoft 365 is stored and processed within the EU and EFTA; limited transfers continue outside it

for remote administration and global security operations, covered by the Standard Contractual Clauses in that Addendum. Review: microsoft.com/privacy

6.2 Disclosure required by law

We may disclose your personal data to law enforcement, regulatory authorities, or courts where we are legally required to do so. We will notify you of any such disclosure where legally permitted.

6.3 Business transfers

In the event of a merger, acquisition, or sale of all or part of our assets, your personal data may be transferred to the acquiring entity. We will notify you before your data is transferred and becomes subject to a different privacy policy.

6.4 Changes to our service providers

We may add, replace, or remove service providers over time. Where a change is material (for example, where a new provider processes your health data or introduces a transfer outside the EEA), we will update this Policy and notify you in accordance with section 14.

7. International data transfers

Piik Labs AB is based in Sweden. Our backend database, all image storage including progress photos and activity photos, our website hosting, our diagnostic data, and our product analytics data are hosted within the European Economic Area (EEA). Some of our service providers are established outside the EEA, including in the United States.

When we transfer personal data outside the EEA, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses approved by the European Commission;
- Transfers to countries covered by an EU adequacy decision, including certification under the EU-U.S. Data Privacy Framework where applicable;
- Supplementary technical and organisational measures where required.

Specifically, transfers to the USA involving Anthropic, RevenueCat, Expo, PostHog, Postmark, Loops, and Vercel (website analytics) are covered by Standard Contractual Clauses, as are the limited transfers Microsoft makes outside the EU Data Boundary for remote administration and security operations. Map requests to Mapbox are processed in the United States and through Mapbox's worldwide content delivery network; these transfers rest on Mapbox's certification under the EU-U.S. Data Privacy Framework and on the Standard Contractual Clauses in its data processing agreement. Xano, Vercel (website hosting, progress photos and activity photos), and Sentry are US-incorporated companies but store our data within the EU, so no transfer of that data outside the EEA takes place. You may request a copy of the applicable safeguards by contacting privacy@bdyctrl.com.

8. Data retention

We retain personal data only for as long as necessary to fulfil the purposes described in this Policy, or as required by law. When you delete your account, we will delete or anonymise your personal data within 30 days, except where retention is required by law.

Data category	Retention period
Account and identity data	Until account deletion, plus a 30-day grace period
Fitness and health data	Until account deletion, or until consent is withdrawn
Progress photos and uploaded images	Until you delete the image or your account
City and country, including per-workout labels	Until account deletion
Coordinates from the city and country check	Not retained. Resolved on-device and discarded.
Routes of recorded activities (your full route and the shared copy)	Until you delete the activity or withdraw your consent to save routes. When your account is deleted, routes are deleted in full within the 30 days set out above.
Activity photos	Until you delete the photo, the activity or your account
Where an activity photo was taken	Until you withdraw your consent to save routes, or delete the photo, the activity or your account
The copy of a photo on a share card	Until you delete the card or your account
Heart rate, active energy and steps from Apple Health	Kept on your device. Not stored by us.
IP address in map requests	30 days, held by Mapbox
Profile ID, interests and language setting	Until account deletion
Push notification token	Until permission is revoked or the account is deleted
Derived data (BDYCharge points, AI insights, generated plans)	Until account deletion
Bolt conversation history	Until you delete the conversation or your account
Community content (posts, comments)	Until you delete the content or your account
Social graph data (follows, interactions)	Until account deletion or the connection is removed
Blocks	Until you remove the block or delete your account
Reports and reported content	Until the report has been reviewed and resolved
Service logs (IP address, request headers)	24 hours
Website visit statistics	24 hours, then aggregate statistics only
Diagnostic and crash data	90 days
Product analytics events	Until account deletion, or up to 7 years where no account is created
Consent records	Until account deletion
Payment and billing records	7 years (Swedish Bookkeeping Act, bokföringslagen)
Support communications	3 years from last contact
Legal hold data	As required by applicable law

9. Your rights under the GDPR

As a data subject in the EU/EEA, you have the following rights. We will respond to all requests within one month.

- **Access (Art. 15)**: obtain a copy of the data we hold about you.
- **Rectification (Art. 16)**: correct inaccurate or incomplete data. Most data can be updated directly in the App.
- **Erasure (Art. 17)**: delete your data. You can delete your account in the App.
- **Restriction (Art. 18)**: limit how we process your data in certain circumstances.
- **Portability (Art. 20)**: receive your data in a structured, machine-readable format.
- **Objection (Art. 21)**: object to processing based on our legitimate interests, and to direct marketing at any time.
- **Withdraw consent (Art. 7)**: at any time, via account or device settings. You withdraw your health and fitness data consent by deleting your account (see section 5). Withdrawal does not affect prior processing.
- **Automated decision-making (Art. 22)**: our AI features do not produce legal or similarly significant effects, but you may request human review of any AI output, express your point of view, and contest it.

To exercise any of these rights, contact privacy@bdyctrl.com. You may also lodge a complaint with the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, IMY) at imy.se, or with the supervisory authority where you live.

10. Cookies and tracking technologies

We do not use advertising cookies, tracking pixels, or retargeting technologies. The App does not use cookies; it uses device-level identifiers as described in section 3.2.

The App stores map tiles from Mapbox (see section 6.1) on your device. Mapbox's usage and location telemetry is switched off in the App.

The bdyctrl.com website sets no cookies and stores nothing in your browser. There is no consent banner because there is nothing to consent to. The site is hosted by Vercel Inc. Server logs generated by hosting (IP address, browser type, and pages requested) are processed to operate and secure the site. We use Vercel Web Analytics to measure visits to the site. It sets no cookies and records the page visited, the referring site, approximate location, and browser, operating system and device type.

The App uses product analytics only with your consent, which you can withdraw at any time in Settings. If we introduce advertising pixels, retargeting, or any other technology requiring consent, we will update this section and implement a consent management solution before any such tracking begins.

11. Children's privacy and minimum age

You must be at least 16 years old to create an account and use the Services. The Services are not directed at children under 16, and we do not knowingly collect personal data from anyone under 16.

We ask for your date of birth during onboarding and use it to confirm that you meet this minimum age. If we become aware that an account has been created by someone under 16, we will delete that account and the associated personal data.

11.1 GDPR Article 8

Article 8 GDPR sets the age at which a child can consent to information society services at 16, and permits individual member states to set a lower age, not below 13. Member state thresholds currently range from 13 to 16. Because our minimum age of 16 is at or above the threshold in every EEA member state, no parental consent mechanism is required for our Services, and we do not process the personal data of any user below the applicable age of consent in their country.

11.2 Children under 13 (COPPA)

The Services are not directed to children under 13, and we do not knowingly collect, use, or disclose personal information from children under 13 as defined by the United States Children's Online Privacy Protection Act (COPPA). If we learn that we have collected personal information from a child under 13, we will delete it promptly.

11.3 Users aged 16 and 17

Users aged 16 and 17 have additional protections in community features, described in section 3.5. If you are under 18, you can remove any content you have posted at any time by deleting it in the App, or ask us to remove it by contacting privacy@bdyctrl.com. Removal does not guarantee complete removal of content that other users have already copied. If you are 16 or 17, we store the route of an activity only after you give the consent to save routes yourself, and the activities you record stay visible only to you (see section 3.5).

11.4 Reporting

If you believe a person under 16 has provided us with personal data, please contact us at privacy@bdyctrl.com and we will investigate and delete that data promptly.

12. Data security

We implement appropriate technical and organisational measures to protect your personal data against unauthorised access, alteration, disclosure, or destruction. These measures include:

- Encryption of data in transit using TLS 1.2 or higher
- Encryption of sensitive data at rest
- Password hashing using industry-standard algorithms
- Row-level access controls so that your data is accessible only to your account
- Role-based permissions for staff access
- Secure token-based authentication
- Regular security reviews and vulnerability assessments

No system is perfectly secure. In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify the relevant supervisory authority within 72 hours and affected users without undue delay, as required by GDPR Articles 33 and 34.

13. App stores

The App is distributed on the Apple App Store. Piik Labs AB is solely responsible for the App and its content; Apple has no obligation to provide maintenance or support. Apple's privacy practices are described at apple.com/legal/privacy.

Apple Health. If you connect Apple Health and give your consent, the App reads workouts with their routes, heart rate, active energy, steps, and walking and running distance from Apple Health, and writes the activities you record in the App to Apple Health as workouts with their route, distance and estimated active energy. You choose which of these to allow in your device's Health settings, and you can change that, or withdraw your consent in Settings, at any time.

We use this data to show heart rate, energy and cadence on your activities, and to add workouts you recorded elsewhere to your training history. Heart rate, active energy and steps are processed on your device and are not sent to us. If you include one of them in an image you share outside the App, it leaves your device in that image. For a workout added from Apple Health, we store its type, date, duration, distance and elevation, and its route if you have consented to saving routes (see sections 3.2 and 8).

Apple Watch. The BDYCTRL app on Apple Watch records your heart rate, distance, active energy and, outdoors, your route, and saves the workout to Apple Health. It does not send data to us. If you have connected Apple Health, a workout recorded on the Watch is added to your history in the App as described above.

Apple Health data is never used for advertising, marketing or data mining, never sold, and never shared with third parties for those purposes, in accordance with Apple's Developer Guidelines.

The App is not currently on Google Play. When it launches there we will submit a Data Safety declaration reflecting this Policy and update this section.

14. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. When we make material changes, we will:

- Update the "Last updated" date at the top of this document;
- Notify you by email if you have an account with us;
- Display a prominent notice in the App;
- Where required by law, seek your renewed consent.

We encourage you to review this Policy periodically. Continued use of the Services after changes take effect constitutes your acceptance of the revised Policy, to the extent permitted by law.

15. Users outside the EEA

The Services are operated from Sweden and are designed around EU data protection standards. If you use the Services from outside the EEA, your personal data will be processed in the EEA and in the other locations described in section 7. Depending on where you live, you may have additional or different rights under local law. Contact us at privacy@bdyctrl.com and we will tell you what rights apply to you and help you exercise them.

If you live in the United States, your state may give you specific rights over your personal data, such as the right to know what we hold, to have it corrected, or to have it deleted. We extend the access, correction, deletion, portability and objection rights described in section 9 to everyone who uses the Services, wherever they live. To exercise any of them, contact us at privacy@bdyctrl.com.

15.1 United States: state privacy laws

Some US states give their residents rights over their personal data, including California, Colorado, Connecticut, Virginia and others. Whichever state you live in, you can ask us to tell you what personal data we hold about you, give you a copy, correct it, delete it, or send it to you in a portable format, as described in section 9.

- We do not sell your personal data, we do not share it for targeted advertising, and we do not use it for profiling that leads to decisions with legal or similarly significant effects on you.
- We process sensitive data, such as the routes of the activities you record and your health and fitness data, only with your consent, and only to provide the Services as described in this Policy. You can withdraw that consent at any time in Settings.
- We do not treat you differently for using any of these rights.
- You can make a request yourself or through an authorised agent. We will confirm the request comes from you, or that the agent acts for you, before we act on it.
- If we turn down a request, you can appeal by writing to legal@bdyctrl.com within 60 days of our answer. We decide an appeal within 45 days and tell you why. If you disagree with the outcome, you can contact your state's Attorney General.

To make a request, write to privacy@bdyctrl.com.

15.2 Consumer health data

If you live in Washington, Nevada or Connecticut, or another US state with a consumer health data law, our Consumer Health Data Policy also applies to you. It sets out which of your data those laws treat as health data, where it comes from, who receives it, and how to use your rights.

16. Governing law and jurisdiction

This Privacy Policy is governed by the laws of Sweden and the European Union, including the General Data Protection Regulation (EU) 2016/679 and the Swedish Data Protection Act (lag (2018:218)).

Any disputes arising from this Policy are subject to the jurisdiction of the Swedish courts, without prejudice to your rights as a consumer under applicable mandatory law in your country of residence.

17. Contact us

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

Company	Piik Labs AB
Organisation number	559577-8506
VAT number	SE559577850601
Address	Box 691, 414 52 Göteborg, Sweden
Privacy enquiries	privacy@bdyctrl.com
Legal and compliance	legal@bdyctrl.com
Supervisory authority	Integritetsskyddsmyndigheten (IMY), imy.se · imy@imy.se

© 2026 Piik Labs AB. BDYCTRL is a Piik Labs brand. All rights reserved.