

BDYCTRL — Privacy Policy

Piik Labs AB · Version 1.1.4

Effective date: 17 August 2026

Last updated: 17 August 2026

Applies to: the BDYCTRL mobile application (iOS) 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
- Email address
- Password (stored in hashed form — we never store plain-text passwords)
- Profile photo (optional)
- Date of birth (used to confirm you meet the minimum age for the Services — see section 11)
- Gender (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
- 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

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.

Location data

When you set up your account, the App checks your device's location once to determine your city and country. The coordinates are resolved to a city and country name on your device and are never transmitted to us or stored. We keep only the resulting city and country. 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; this stops us using your city and country, but it does not revoke the device permission itself. We do not access your location in the background, during workouts, or at any other time.

Your city and country set your profile location. When community features launch, they will also be used to match you with local challenges and groups. Community features are not yet live — see 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.

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

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 once community features are live.
- **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

Community features are not yet live. This section describes how they will work. We will notify you and update this Policy before they become available.

When you share content — posts, comments, reactions, progress photos, or workout summaries — we store that content and the metadata attached to it, such as timestamps and interaction counts. We also store your connections (who you follow and who follows you), your participation in challenges, and your leaderboard positions.

Sharing is always an active choice; nothing is posted automatically. Shared posts are visible to other BDYCTRL users in the feed. You can post in anonymised mode, which replaces your username and profile photo with a generic identity. You can delete your content at any time, though where other users have already interacted with it, traces of that interaction may remain on their accounts.

We do not sell or licence your content or your social connections to third parties.

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	Date of birth	Art. 6(1)(c) — legal obligation
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, chat messages	Art. 6(1)(b) — contract Art. 9(2)(a) — explicit consent
Set your city and country	City and country, derived on-device from a one-time location check at signup	Art. 6(1)(a) — consent (device permission)
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 and social feed	Social graph, content, interaction data	Art. 6(1)(b) — contract Art. 6(1)(a) — consent where required
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	Art. 6(1)(f) — legitimate interest
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 only with your explicit, informed consent. During onboarding you are presented with a clear consent request specifically covering health and fitness data, including its processing by our AI features. You may withdraw this consent at any time through your account settings. Withdrawal of consent does not affect the lawfulness of processing that occurred before withdrawal.

Withdrawal of consent to health data processing will limit our ability to provide core features of the Services, including workout tracking, analytics, and AI plan generation.

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 you upload from the App. Progress photos are held in private storage that is not publicly accessible and is retrievable only through an authenticated request from your own account. All data is stored in the EU region. Data processing agreement in place.

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. 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. 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

We do not use any third-party product analytics service. We 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, our website hosting, and our diagnostic 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, Postmark, and Loops are covered by Standard Contractual Clauses, as are the limited transfers Microsoft makes outside the EU Data Boundary for remote administration and security operations. Xano, Vercel, 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	Until account deletion
Device coordinates	Not retained. Resolved on-device and discarded.
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
Diagnostic and crash data	90 days
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. 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 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 do not run any website analytics service.

If we introduce analytics, 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 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.

The App does not currently integrate with Apple Health (HealthKit) and does not read or write any HealthKit data. We plan to offer this integration in a future release. It will be optional, and we will update this Policy before it becomes available. Where enabled, HealthKit data will never be used for advertising, sold, or shared with third parties for marketing, 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.

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.