



UPTIVO PRIVACY POLICY

Version r2605.10 — Effective Date: August 31, 2026

This Privacy Policy describes how **UPTIVO S.r.l.** ("UPTIVO", "we", "us") collects, uses and protects personal data of users of: (i) the UPTIVO website at www.uptivo.fit and any related domain; (ii) the UPTIVO mobile and web applications; and (iii) any UPTIVO service. This Privacy Policy applies regardless of how you access the Services. Where you access the Services as an end user of a Customer (e.g. a fitness club using UPTIVO under a Service Agreement), an additional layer of contractual arrangements applies between UPTIVO and that Customer (see Section 11).

1. DATA CONTROLLER AND CONTACT

UPTIVO S.r.l., registered office at Via L. Vitali 1, 20122 Milano (MI), Italy, VAT IT08849150969, certified email (PEC) euvic@legalmail.it, is the Data Controller of your personal data within the meaning of Article 4(7) GDPR.

For privacy queries (including requests to exercise your rights under Section 6) you may contact us at support@uptivo.fit or by post at the registered office above.

2. CATEGORIES OF PERSONAL DATA

We collect and process the following categories of personal data, to the extent necessary for the purposes described in Section 3.

2.1 Identification and contact data: name, surname, nickname, profile image; email address; telephone number; mailing address; tax identifier where required for billing.

2.2 Account and authentication data: UserId; username; hashed and salted password; JWT authentication tokens; API keys; OAuth device identifiers.

2.3 Demographic and profile data: date of birth; gender; language; country; time zone; occupation.

2.4 Fitness profile and preferences: weight; height; training goals; injury history; activities to avoid; weekly availability; notification, ranking and calendar preferences.

2.5 Club and subscription data: club affiliation; role (athlete or staff); licenses; credits; class bookings.

2.6 Device and sensor data: hardware identifier; device model; sensor name; paired bridge devices and SNAP; application identifiers.

2.7 External account integrations: connection identifiers and OAuth access tokens for third-party services such as Garmin Connect, Stripe, PayPal, Whoop and Withings.

2.8 Usage and technical data: login records; IP address; session timestamps; device identifiers; User Agent; diagnostic logs and Application Insights metrics.

2.9 Health and biometric data — special category under Article 9 GDPR. The Services involve the processing of **data concerning health** within the meaning of Article 4(15) GDPR. This includes: (a) heart-rate metrics (minimum, maximum, average and resting), heart-rate zones, target thresholds, heart-rate variability (HRV), SpO2; (b) Body Mass Index (BMI), Functional Threshold Power (FTP); (c) training and performance telemetry (date and time, duration, distance, calories, power, cadence, hits, geolocation, altitude, elevation gain); (d) integrated health data from third-party providers (steps, stress, body battery, sleep stages, respiration, training plans); (e) clinical and body-measurement data where provided by you or by a Customer (blood pressure, blood glucose, body composition, fitness test results); (f) Nate AI-generated feedback derived from your profile, sleep and HRV data. These categories qualify as **special categories of personal data** under Article 9 GDPR and are processed only on the legal basis described in Section 4.

2.10 Communications: support requests and related correspondence.

2.11 Payment-related identifiers: identifiers handled by the payment processor. UPTIVO does not store full payment-card data; full payment-card data is processed directly by Stripe and PayPal under their own privacy notices.

3. PURPOSES OF PROCESSING

We process your personal data for the following purposes: (a) **provision of the Services:** account registration, authentication, training session management, dashboards, leaderboards, badges, notifications; (b) **personalization:** computation of heart-rate zones, calorie estimates, points and ranking; (c) **club management:** relationship between athletes and trainers, bookings, operational communications; (d) **Nate AI functionality:** generation of personalized performance evaluations and recommendations based on your profile, sleep and HRV (see Section 5); (e) **customer support:** responding to support requests and managing complaints; (f) **security and maintenance:** diagnostic logging, fraud prevention, abuse prevention, audit logging; (g) **billing and invoicing:** issuing invoices, managing payments, accounting; (h) **compliance with legal obligations:** tax obligations, record-keeping, responses to lawful requests by public authorities; (i) **marketing communications** (only with your prior consent): newsletters and information about UPTIVO services.

What we do not do. We do not use your account, training or health data for advertising profiling, we do not sell identifiable personal data, including health and biometric data, to third parties for their independent commercial purposes, and we do not share your data with third parties for their independent marketing purposes.

4. LEGAL BASIS

We rely on the following legal bases under Article 6 GDPR (and, where applicable, Article 9 GDPR):

- (a) Provision of the Services, personalization, club management, customer support — **Article 6(1)(b) GDPR:** performance of the contract to which you are a party (the Service Agreement or its end-user equivalent).
- (b) Processing of **health and biometric data** (Section 2.9) for fitness, performance monitoring and Nate AI functionality — **Article 9(2)(a) GDPR:** explicit consent, given at registration or when activating health-data features. You may withdraw your consent at any time without affecting the lawfulness of processing carried out before withdrawal; withdrawal will result in the discontinuation of the affected features.
- (c) Nate AI profiling — **Article 6(1)(a) + Article 9(2)(a) GDPR:** explicit consent (see also Section 5).
- (d) Security, fraud prevention, abuse prevention — **Article 6(1)(f) GDPR:** legitimate interest in protecting the integrity of the Services and our users.
- (e) Billing, accounting, tax compliance — **Article 6(1)(b) and 6(1)(c) GDPR:** contract and legal obligations.
- (f) Compliance with other legal obligations — **Article 6(1)(c) GDPR.**
- (g) Marketing communications — **Article 6(1)(a) GDPR:** consent, freely revocable at any time via the unsubscribe link in the communication or via the privacy contact in Section 1.

5. AUTOMATED DECISION-MAKING AND PROFILING (NATE AI)

The Services include the **Nate AI** feature, which uses an artificial-intelligence model to generate personalized performance evaluations and recommendations based on your profile data, heart-rate variability and sleep data. This functionality constitutes **profiling** within the meaning of Article 4(4) GDPR.

Logic, significance and consequences. Nate AI processes the inputs listed above through a generative language model that produces textual recommendations relating to training, recovery and performance. The output is intended to support self-monitoring and is delivered exclusively in informational form.

UPTIVO considers that Nate AI does not fall within the scope of Article 22(1) GDPR, on the basis that the recommendations are **informational and not binding**, are intended to support but not replace your own judgement and the judgement of qualified professionals, and do not condition the provision of any Service.

You have the right at any time to: (i) **disable Nate AI** in your account settings; (ii) **request human intervention** to review any Nate AI output that you consider inaccurate or unsuitable; (iii) **express your point of view and contest** the output. Requests for human intervention are handled by qualified personnel and addressed within a reasonable time and in any event within **thirty (30) days**. To exercise these rights please contact us as described in Section 6.

Nate AI does not output medical advice. The Services are not a medical device under Regulation (EU) 2017/745. You should consult a qualified medical professional before relying on any Nate AI output for health-related decisions.

6. DATA SUBJECT RIGHTS

You have the following rights under Articles 15 to 22 GDPR:

- (a) Right of **access** (Article 15): to obtain confirmation of whether your data is processed and a copy of the data;
- (b) Right of **rectification** (Article 16): to correct inaccurate or incomplete data;
- (c) Right to **erasure / right to be forgotten** (Article 17): to request deletion of your data, subject to exceptions provided by law;
- (d) Right to **restriction** of processing (Article 18): to limit processing in specified circumstances;
- (e) Right to **data portability** (Article 20): to receive your data in a structured, commonly used and machine-readable format and to transmit it to another controller;
- (f) Right to **object** (Article 21) to processing based on legitimate interest, including for direct marketing purposes;
- (g) Right not to be subject to **automated decision-making** (Article 22): see Section 5;
- (h) Right to **withdraw consent** (Article 7(3)) at any time, without affecting the lawfulness of processing carried out before the withdrawal.

How to exercise these rights. You may use the in-app account management functions where available (Settings > Account > Manage / Delete Account), or contact us at support@uptivo.fit. We may need to verify your identity before responding. We will respond without undue delay and in any event within **thirty (30) days** of receipt of the request, in accordance with Article 12 GDPR; this period may be extended by up to two further months for complex or numerous requests, and we will inform you of any such extension.

Account deletion. Upon a deletion request, an automated process removes account credentials, profile images, external-account connections and all telemetry data (heart-rate, geolocation, power, cadence and hits) within thirty (30) days. Backups containing your data are subsequently overwritten according to standard backup-rotation periods. Data we are required to retain for billing, accounting or other legal obligations is preserved for the periods set out in Section 7 and is then deleted.

Right to lodge a complaint. You have the right to lodge a complaint with the Italian Data Protection Authority (Garante per la protezione dei dati personali, www.garanteprivacy.it) or with the supervisory authority of your habitual residence, place of work or place of the alleged infringement.

7. RETENTION PERIODS

We retain your personal data only for as long as necessary for the purposes described above:

- Active user account data: **duration of the subscription**;
- Pending or unconfirmed user registrations: **fifteen (15) days**;
- Unaccepted invitation and registration links: **fifteen (15) days**;
- Device or application registration requests: **seven (7) days**;
- In-app notifications: **sixty (60) days**;

- Diagnostic and error logs: **two (2) months**;
- Security event logs (access, authentication, anomaly detection): **six (6) months**;
- Billing and accounting records: **ten (10) years** from issuance, pursuant to Article 2220 of the Italian Civil Code;
- Records related to a deletion request: telemetry and account data deleted **within thirty (30) days**; backup overwrites follow standard rotation.

After the retention period, your personal data is either deleted or anonymized, except where retention is required by applicable law.

8. INTERNATIONAL TRANSFERS

We process your personal data within the European Economic Area (EEA), with primary storage on servers located in the **Netherlands, Ireland and Germany**.

Where personal data is transferred outside the EEA in connection with the Services (in particular through the third-party processors located in the United States listed in Section 9), we rely on: (a) the **EU-US Data Privacy Framework** (Commission Implementing Decision (EU) 2023/1795) where the recipient is a certified participant; or (b) the **Standard Contractual Clauses** adopted by Commission Implementing Decision (EU) 2021/914, supplemented, where necessary, by additional technical and organizational measures assessed on a case-by-case basis through a Transfer Impact Assessment, available upon request.

9. THIRD-PARTY PROCESSORS

UPTIVO uses the following third-party processors to provide the Services. UPTIVO maintains a data processing agreement with each of them under Article 28 GDPR. The list is updated from time to time and the latest version is available on request.

Processor	Service	Location / Transfer	Categories of Data Transferred
Supabase Inc.	Database, storage, authentication	EU (Ireland)	Account, profile, fitness profile, telemetry, health data
Microsoft Corporation (Azure)	Cloud hosting, infrastructure and Application Insights	EU (Netherlands, Ireland, Germany)	All processing data, diagnostic logs
Microsoft Corporation (M365)	Business email and collaboration	EU	Communications, contact data
OpenAI, L.L.C.	AI / LLM processing (Nate AI)	United States — EU-US DPF	Profile, HRV, sleep data and derived prompts
Google LLC (Gemini)	AI / LLM processing (Nate AI)	United States — EU-US DPF	Profile, HRV, sleep data and derived prompts
Stripe Payments Europe, Ltd.	Payment processing for subscriptions	EU (Ireland)	Identification, contact, payment identifiers (no health data)
PayPal (Europe) S.à r.l. et Cie, S.C.A.	Payment processing for club services	EU (Luxembourg)	Identification, contact, payment identifiers (no health data)
Garmin International, Inc.	Wearable integration (Garmin Connect)	United States — EU-US DPF	OAuth identifiers, fitness and health telemetry
WHOOP, Inc.	Wearable integration (Whoop)	United States — EU SCCs	OAuth identifiers, fitness and health telemetry
Withings SAS	Wearable and connected-health-device integration	EU (France)	OAuth identifiers, body measurement and health data

10. COOKIES AND SIMILAR TECHNOLOGIES (WEBSITE)

The UPTIVO website uses cookies and similar technologies. We distinguish between: (a) **strictly necessary cookies** (no consent required), used to operate the website (session management, security, load balancing); (b) **analytics cookies** (consent required), used to understand how visitors interact with the website on aggregate and anonymized basis; (c) **marketing cookies** (consent required), used to deliver UPTIVO communications across channels and to build advertising audiences on third-party platforms such as LinkedIn, where applicable.

On your first visit to the website you will be presented with a cookie banner from which you can grant or refuse consent on a per-category basis. You can change your preferences at any time via the cookie preference center accessible from the footer of the website.

The UPTIVO mobile application does not use cookies; it uses the platform-specific local storage required for the application to function.

11. END USERS WHO ACCESS THE SERVICES VIA A CUSTOMER

Where you access the Services as an end user of an UPTIVO Customer (for example, as a member of a fitness club using UPTIVO under a Service Agreement), the **Customer is the Data Controller** of your personal data and **UPTIVO is the Data Processor** within the meaning of Article 28 GDPR. The processing is governed by a Data Processing Agreement (DPA) entered into between the Customer and UPTIVO.

In this scenario: (i) authorized staff of the Customer (e.g. trainers, club managers) may view and edit your profile (email, age, heart-rate zones) and monitor your training progress; (ii) the Customer is responsible for the accuracy and lawful use of any data it modifies; (iii) you can interrupt the sharing at any time by removing the club association from the application; (iv) for requests relating to your data you may contact the Customer directly or contact UPTIVO at the privacy contact in Section 1, and we will assist the Customer in responding.

For the Nate AI functionality, the consent to the processing of health data pursuant to Article 9(2)(a) GDPR is collected directly by UPTIVO from the end user, who acts as autonomous data subject for this specific purpose.

12. CHILDREN

The Services are not directed at children under the age of **fourteen (14)**. Pursuant to Article 8 GDPR and Italian Legislative Decree 196/2003 (as amended), if you are under fourteen (14) you may not use the Services without the consent and supervision of a parent or person holding parental responsibility. If we become aware that we have collected personal data from a child under fourteen (14) without verified parental consent, we will delete that data without undue delay. Where the Services are accessed by users residing in jurisdictions setting a different minimum age for digital consent under applicable law, that age applies in lieu of the threshold above.

13. SECURITY

UPTIVO implements technical and organizational measures appropriate to the risk of the processing, in accordance with Article 32 GDPR, including: encryption of personal data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent); role-based access control and multi-factor authentication for administrative and privileged access; network segregation and firewall controls; regular operating-system and application updates; automated regular backups with off-site replication; documented disaster-recovery and business-continuity procedures; logging and monitoring of relevant security events; confidentiality undertakings for personnel with access to personal data; periodic vulnerability monitoring and security review of changes to production systems.

In the event of a Personal Data Breach, UPTIVO will notify the competent supervisory authority pursuant to Article 33 GDPR where required. Where the breach is likely to result in a high risk to your rights and freedoms, we will notify you without undue delay in accordance with Article 34 GDPR.



14. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. The current version is identified by the version number and effective date in the footer of each page. For material changes, we will notify you through the Services or by email at least **thirty (30) days** before the changes take effect.

15. CONTACTS

Privacy queries: **support@uptivo.fit**

Certified email (PEC): **euvic@legalmail.it**

Postal address: **UPTIVO S.r.l., Via L. Vitali 1, 20122 Milano (MI), Italy**

Italian Data Protection Authority: **www.garanteprivacy.it**