

PRIVACY NOTICE

TrintendLab platform (app.trintend.com) — for athlete users

Version 1.0 – in force from 23 August 2026

1. The controller

Controller: **Viktor Kovács**, sole trader under Hungarian law (Hungarian: *egyéni vállalkozó*)

Registered office / postal address: Hérics utca 16., 1112 Budapest, Hungary

Register: Hungarian register of sole traders, maintained by the Ministry of the Interior

Tax number: 45715473-1-43

Contact for data protection matters: info@trintend.com

Telephone: +36 20 310 7716

Data protection officer. No data protection officer has been appointed. The controller has assessed Article 37(1) GDPR: it is not a public authority or body; its core activities do not consist of processing operations which by their nature, scope or purposes require regular and systematic monitoring of data subjects on a large scale; and the processing of health data described in this notice is not carried out on a large scale within the meaning of Article 37(1)(b) and (c). Hungarian law, which governs the controller as an entity established in Hungary, imposes no additional appointment threshold. This assessment is reviewed as the service grows, and this notice is updated if the position changes. Data protection enquiries are handled at the address above.

The controller is established in Hungary. Its lead supervisory authority is the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

2. Purpose and scope of this notice

This notice explains how the TrintendLab platform (the "Platform", app.trintend.com) processes the personal data of its athlete users (the "Data Subject"), under Regulation (EU) 2016/679 (GDPR).

3. Key terms

Term	Meaning
Personal data	Any information relating to an identified or identifiable natural person.
Special category data	Data concerning health — here: laboratory results, physiological metrics derived from them, reported injuries and health conditions, and the heart rate variability (HRV), resting heart rate and sleep duration read from Intervals.icu — to which the GDPR applies stricter rules requiring explicit consent.
Controller	The party determining the purposes and means of processing (here, the operator of the Platform).

Term	Meaning
Processor	A party processing personal data on behalf of and on the instructions of the controller (see clause 6).

4. Categories of data, purposes and legal bases

Category	Specific data	Purpose	Legal basis
Account / registration	Email address, password (hash), role, language setting	Account creation, identification, access management	Performance of a contract (Art. 6(1)(b)); the registration declaration itself: consent (Art. 6(1)(a))
Athlete basic data	Name, sport, training history, goals, weekly session counts	Personalisation of the training plan	Performance of a contract
Laboratory results and physiological metrics	Uploaded exercise test reports, metrics extracted from them by AI analysis, metabolic model, training zones	Training plan generation, performance analysis	Explicit consent (Art. 9(2)(a)) + performance of a contract
Reported health information	Injuries, health conditions, load limitations	Safe personalisation of the training plan	Explicit consent (Art. 9(2)(a))
Training plans and sessions	Generated training plans, session content, completion status	Provision of the ordered service	Performance of a contract
Training and wellness data read from Intervals.icu	Activities actually completed (type, duration), heart rate variability (HRV), resting heart rate, sleep duration	Comparison of plan against actual performance, evaluation of recovery	Explicit consent (Art. 9(2)(a)) + performance of a contract
Daily evaluation and weekly summary	AI-generated evaluation text, the plan-versus-actual comparison, a snapshot of the wellness data, the name of the AI model used	Daily feedback to the Athlete; basis for the next training plan	Explicit consent + performance of a contract
Avatar chat and fault reports	Messages exchanged between the Athlete and the AI avatar, structured fault report fields, redacted context formed from the most recent messages	Provision of AI-based coaching interaction; technical investigation of reported faults	Performance of a contract + legitimate interest (service quality and fault diagnosis)
Service usage and entitlement data	Service package purchased, start and end date of the training block, regenerations used, daily avatar token usage	Enforcement of purchased entitlements, abuse and cost control	Performance of a contract + legitimate interest

Category	Specific data	Purpose	Legal basis
Payment data	Transaction amount, date, invoicing status, billing name and address, billing email address, billing country; the card number, expiry date and security code are not stored by the Platform and are handled by Stripe	Payment processing, invoicing	Performance of a contract + legal obligation (accounting/tax)
Location evidence for VAT purposes	Country of the billing address and the issuing country of the payment card , as reported by Stripe, together with whether the two agree	Determination of the place of supply for VAT: EU VAT law requires two independent, non-contradictory items of evidence of the customer's location	Legal obligation
Consent records	The type of consent, whether it was given or withdrawn, the timestamp, the version of the text presented, and — where the declaration is made through a web request — the IP address and user agent	Demonstrating compliance with Article 7(1) GDPR and evidencing the declaration under clause 10.2 of the Terms	Legal obligation (Art. 7(1)) + legitimate interest (evidence)
Athlete credentials	The Athlete's Intervals.icu API key — stored encrypted, never returned to the client	Operation of the synchronisation service	Performance of a contract
Technical logs	Sign-in and system event logs (audit log), IP address, user agent	Security, abuse prevention, evidence of legally relevant events	Legitimate interest + legal obligation

A note on the consent record. For the declaration made at the point of purchase (the acknowledgment that performance begins immediately), the Platform also records the IP address and user agent. For the data protection declaration made at **registration**, those two items are not available, because the record is written inside the database transaction that creates the account, without access to the HTTP request. The timestamp and the version of the text are recorded in both cases.

5. Automated processing and artificial intelligence

The Platform uses artificial intelligence (Anthropic Claude models) to generate training plans, analyse uploaded laboratory reports, provide avatar-based coaching interaction, produce the daily evaluation and weekly summary and, where a fault is reported, to carry out technical diagnostics.

The Platform may use different AI models for different sub-tasks and may change the set of models in line with technological developments. A change of model affects neither the purpose nor the legal basis of processing; the processor (Anthropic) remains the same.

An AI-generated training plan, daily evaluation or avatar response does not constitute a decision based solely on automated processing which produces legal effects concerning the Data Subject or similarly significantly affects them within the meaning of Article 22 GDPR. The sport-science content is advisory: the Data Subject decides freely whether

to follow it, may depart from it at any time, may request a full regeneration of the plan within the limits of their Service Package, and may raise any objection to the outcome at info@trintend.com, where it is reviewed by a person.

The fault-reporting agent reads source code (not personal data) when investigating a report; the context formed from the most recent messages is redacted before processing (removal of API-key-like and other sensitive patterns).

The Platform does not use personal data to train or fine-tune artificial intelligence models, and does not permit its AI processor to do so.

6. Processors, recipients and transfers

The Platform uses the processors and recipients listed below.

Provider	Role	Data processed	Location / transfer basis
Supabase Inc.	Database, authentication, file storage	All stored categories listed in clause 4	Stored in the EU — Ireland (AWS eu-west-1); operator established in the USA — EU–US Data Privacy Framework / standard contractual clauses
Vercel Inc.	Application hosting, runtime	All data passing through the application (in transit)	USA — EU–US Data Privacy Framework / standard contractual clauses
Stripe, Inc. / Stripe Payments Europe, Ltd.	Payment services	Payment and billing data	Ireland and USA — EU–US Data Privacy Framework / standard contractual clauses
Billingo Zrt.	Invoicing (Hungarian tax-authority-compatible) and delivery of the invoice by email	Billing data, billing email address, content of the invoice	Hungary — EU
Anthropic PBC (Claude API)	AI plan generation, laboratory analysis, avatar conversation, daily evaluation, weekly summary, fault diagnostics	Athlete, training plan and conversation data passed to the model	USA — standard contractual clauses
INTERVALS.ICU LTD	Training data synchronisation; source of actual activities and wellness data	Zone and plan data sent; activity, HRV, resting heart rate and sleep data read — tied to the Athlete's own Intervals.icu account	Company registered in the United Kingdom (company no. 13083695, 71–75 Shelton Street, London WC2H 9JQ); service operated on servers located in Germany. Transfers to the UK rest on the European Commission's adequacy decision for the United Kingdom.

Provider	Role	Data processed	Location / transfer basis
Hostinger International Ltd.	Email delivery (SMTP) of the order confirmation, invoices, the daily evaluation email and other platform notifications; hosting of the marketing website	Recipient email address, content of the email	Cyprus — EU. Hostinger uses sub-processors outside the EU for mail delivery and security filtering, including MailChannels (Canada — adequacy decision) and Proofpoint and Cloudflare (USA — EU-US Data Privacy Framework / standard contractual clauses). The email path is therefore not EU-only.
GitHub, Inc.	Code storage; read-only code access by the fault-reporting agent	Source code only — no athlete data is placed in the repository	USA — EU-US Data Privacy Framework / standard contractual clauses

Where the Athlete does not have a coach on the Platform, no third party other than the processors listed above has access to the Athlete's training plans or health data.

Personal data are not sold, and are not disclosed to any recipient for advertising purposes.

7. Transfers to third countries

Some of the providers listed in clause 6 are established in, or also process data in, a country outside the European Economic Area. Those transfers rest on Chapter V GDPR: on an adequacy decision of the European Commission where one covers the country concerned (the United Kingdom and Canada), and otherwise on certification under the EU-US Data Privacy Framework or on standard contractual clauses approved by the European Commission, as stated provider by provider in the table above.

The database and file storage (Supabase) operate within the European Union, in the Irish region; athletes' health data are therefore stored in the EU. Stored data are nevertheless transferred to a third country during application execution (Vercel) and AI processing (Anthropic).

A copy of the safeguards relied on for a specific transfer is available on request at info@trintend.com.

8. Retention

The Platform's guiding rule is that data tied to an account are kept for as long as the account exists, and are removed when the account is deleted.

Data	Retention
Account data, athlete profile	For the lifetime of the account, subject to clause 9
Laboratory results, physiological metrics, training zones	For the lifetime of the account, since they form the basis of further training plans; the effect of withdrawing consent is described in clause 10
Training plans, sessions, weekly summaries, daily evaluations and the wellness snapshot stored with them	For the lifetime of the account

Data	Retention
Avatar conversations and fault reports	For the lifetime of the account
Service usage and entitlement data	For the lifetime of the account
Technical logs / audit log	For the lifetime of the account; entries evidencing a legally relevant declaration (consent, the acknowledgment given at purchase, a refund) are retained for the limitation period applicable to claims under the contract
Consent records	For the duration of the processing based on the consent and for the limitation period thereafter, as Article 7(1) GDPR requires the controller to be able to demonstrate that consent was given
Billing and payment data	8 years, as required by Hungarian accounting and tax law
Location evidence for VAT purposes	10 years from the transaction, as required by Article 24b of Implementing Regulation (EU) No 282/2011; anonymised rather than deleted on an erasure request (clause 9)

The Platform does not currently apply a separate, shorter automated deletion period to daily evaluations, avatar conversations, usage data or audit logs; those records live and die with the account. A Data Subject who wishes a specific record removed sooner may request erasure at any time under clause 10, and the Platform gives effect to it subject only to clause 9.

Expiry of the four-week training block limits the availability of services but does not by itself entail deletion of any data.

9. Erasure requests and the legal retention exception

Where a Data Subject requests erasure and a billing reference still subject to a legal retention obligation is attached to that Athlete, the Platform **anonymises** the data concerned rather than deleting it outright, in such a way that the accounting retention obligation is satisfied but the Data Subject is no longer identifiable from it.

10. Rights of the Data Subject

- **Access** (Art. 15): to obtain confirmation as to whether personal data are processed and, if so, access to them.
- **Rectification** (Art. 16) of inaccurate data.
- **Erasure** (Art. 17), subject to clause 9.
- **Restriction** of processing (Art. 18).
- **Objection** (Art. 21) to processing based on legitimate interests.
- **Data portability** (Art. 20): to receive data processed by automated means on the basis of contract or consent in a structured, machine-readable format.
- **Withdrawal of consent** (Art. 7(3)) at any time, without retroactive effect.

How withdrawal works. Withdrawal is self-service and is exercised **separately for each processing purpose**, from the "Data protection" page in the Athlete's account. No message to the Platform is required, and withdrawal is as easy as giving consent. Withdrawal has real, immediate consequences:

- **Intervals.icu synchronisation.** Withdrawing this consent deletes the stored access key and ends the reading of activity, HRV, resting heart rate and sleep data.
- **Laboratory results and health information.** Withdrawing this consent stops the physiological metrics derived from laboratory results being used in further training plan generation, in the daily evaluation and in the weekly summary. Laboratory reports already uploaded are **not** deleted by the withdrawal; their deletion is a separate request under Article 17, which deleting the account also achieves.
- **The registration declaration** cannot be withdrawn while the account exists, because the Platform cannot operate the account without processing the account data; deleting the account is the route, and it is available at any time.
- **The acknowledgment given at the point of purchase** (that performance begins immediately) is a contractual declaration, not a consent to processing, and is therefore not withdrawable through this page; the right of withdrawal under the Terms is exercised as described there.

Withdrawal does not affect the lawfulness of processing carried out on the basis of the consent before it was withdrawn. Where a withdrawal means a purchased service can no longer be provided in full, the Terms describe the consequence.

Requests under this clause should be sent to info@trintend.com. The Platform responds without undue delay and in any event within one month.

11. Remedies

A Data Subject may lodge a complaint with the supervisory authority of their habitual residence, place of work or place of the alleged infringement (Article 77 GDPR), or with the controller's lead authority, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH, 1055 Budapest, Falk Miksa utca 9–11; postal address: 1363 Budapest, Pf. 9; naih.hu). A Data Subject also has the right to an effective judicial remedy.

12. Cookies and storage on the user's device

The application at app.trintend.com stores on the user's device only information that is **strictly necessary** to provide the service the user has expressly requested:

- the **sign-in session cookie**, without which an authenticated area is not possible, and
- a **language cookie** (`NEXT_LOCALE`), which records the chosen interface language.

No consent is required for this storage, and no consent banner is shown. The application sets **no** analytics, tracking, profiling or advertising cookies and embeds no third-party analytics or advertising services. If that changes, a consent mechanism will be introduced first and this clause updated.

This notice covers the application. The marketing website at www.trintend.com has its own privacy notice.

13. Security measures

The Platform stores particularly sensitive credentials — including the Athlete's Intervals.icu API key — using AES-256-GCM encryption, in such a way that they are never returned to the client side. SMTP access and other provider secrets live only in encrypted environment variables of the runtime, never in the database.

The Platform applies database-level, row-level access control (RLS) to ensure that each Data Subject can access only their own data. Security- and legally-relevant events (sign-in, permission change, legal declaration, consent, withdrawal, refund) are recorded in an audit log. Where a processing step depending on consent cannot verify that consent, it is refused rather than allowed to proceed.

14. Amendment of this notice

The Platform may amend this notice. Data Subjects will be informed of a material amendment through the Platform or by email. The version and date appear at the head of this document.