Data Processing Addendum

Last updated: 2026-09-29 · Version 2026-09-29 (updated from 2026-09-28: documented the POPIA section 72 basis for the cross-border transfer to Supabase's EU hosting — previously flagged as needing confirmation)

1. Purpose of this Addendum

Section 21 of South Africa's POPI Act requires a Responsible Party to have a written agreement with any Operator that processes personal information on its behalf, setting out the Operator's security obligations. This Addendum is that agreement between your Organization (the **Responsible Party**) and Vantic (the **Operator**). It supplements, and does not replace, our Privacy Policy and Subscription Agreement — where any of these conflict on data-processing terms specifically, this Addendum governs.

2. Roles

Your Organization decides what player and staff data to enter into Vantic, and why — you are the Responsible Party. Vantic processes that data only on your Organization's documented instructions (this Addendum, the Subscription Agreement, and your Organization's own configuration of the platform), for the purposes stated in section 3 below, and not for any other purpose. Vantic never acts as a Responsible Party for player or staff data.

3. Scope, nature, and purpose of processing

Category of data subject	Personal information processed	Purpose
Organization staff (coaches, S&C)	Name, email, role, assigned teams	Account access and platform administration
Players (predominantly minors)	Name, date of birth, gender, age group, team/position, physical test results, wellness scores, injury/recovery records	Performance testing, scoring and benchmarking, wellness monitoring, injury/return-to-play tracking, automated program generation

This mirrors the categories described in our PAIA/POPIA Manual and Privacy Policy, section 2 — nothing here expands what Vantic collects or why.

4. Operator's obligations

- Process personal information only on your Organization's instructions, and only for the purposes in section 3 — never to build products for other customers, train a shared model, or for advertising (see Privacy Policy, section 3).
- Keep personal information confidential — Vantic staff and any sub-processor are bound by confidentiality obligations covering this data.
- Put in place, and maintain, the security measures described in section 6 below.
- Not engage a new sub-processor without notifying your Organization first (section 5).
- Assist your Organization in responding to a data subject access, correction, or deletion request, to the extent the request concerns data Vantic holds on your Organization's behalf.
- Notify your Organization without delay if Vantic becomes aware of a security compromise affecting your data, so your Organization can meet its own notification obligations under POPIA sections 21 and 22.
- Return or delete personal information on termination, per section 8 below.

5. Sub-processors

Vantic uses the following sub-processors, each under its own contract:

- **Supabase** — database, authentication, and file storage hosting.
- **PayFast** — payment processing, once billing is live (not yet active). Only billing-relevant information is shared; player data is never sent to PayFast.

Vantic will notify your Organization before adding a new sub-processor that will process your Organization's personal information, giving your Organization the opportunity to object on reasonable data-protection grounds.

6. Security measures

Real measures in place, most recently verified 2026-08-12 (RLS coverage has continued to expand with every migration since — 109 migrations applied as of this update, all following the same row-level-security-first pattern):

- Row-level security enforced at the database level across every table holding player/organization data — one Organization's staff cannot access another Organization's data, enforced by the database itself, not just the application.
- All server-side functions performing privileged actions verify the caller's identity before doing anything.
- Data encrypted in transit (HTTPS/TLS) and at rest (AES-256, automatic via Supabase's infrastructure).
- No passwords or API keys stored in the application's source code.

Multi-factor authentication is not yet offered to Vantic staff accounts, though the underlying platform (Supabase Auth) supports it — disclosed here as a real, currently open gap, consistent with our Privacy Policy, section 9, not glossed over for this Addendum.

7. Data subject rights

Requests from a player, parent/guardian, or staff member about their own data should go to your Organization first, since your Organization holds the direct relationship — Vantic will support your Organization in fulfilling any valid request, including by providing access to, correcting, or deleting the relevant data on your Organization's instruction.

8. Return or deletion of data on termination

This mirrors our Privacy Policy, section 7, exactly — it is not a separate policy: your Organization can export its data at any time while its subscription is active or within 90 days of cancellation. After that window, player- and staff-identifying fields are permanently deleted; numeric test and wellness results are kept only in de-identified form. Your Organization can request full deletion, including of de-identified data, at any time, rather than waiting for the 90-day window.

9. Cross-border transfer

Vantic's production data is hosted with Supabase in the eu-north-1 (Stockholm, Sweden) AWS region — personal information is transferred outside South Africa for processing and storage. **The basis for this transfer, under POPIA section 72(1)(a),** is Supabase's own Data Processing Addendum (effective automatically on acceptance of Supabase's terms, published at supabase.com/legal/dpa), which

incorporates the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) under Module Three (processor to processor, since Vantic acts as an Operator/processor for each Organization and Supabase is Vantic's sub-processor). Those Clauses impose data protection obligations substantially similar to POPIA's own conditions, including restrictions on Supabase transferring data onward to any further country — the two elements POPIA section 72 requires of a qualifying binding agreement.

10. Records and audit

Vantic will, on reasonable written request and no more than once per 12 months (or promptly following an actual security compromise), provide your Organization with reasonable information about the security measures in place to demonstrate compliance with this Addendum. Vantic is currently a single-founder company without a dedicated compliance team — a full on-site audit right is not offered at this stage; this will be revisited as the Company grows.

11. Liability

Liability under this Addendum is subject to, and does not create any liability pool separate from, the limitation of liability set out in the Subscription Agreement — that same aggregate cap applies to claims arising under this Addendum, not an additional or separate amount. As between the parties, Vantic remains responsible to your Organization for a security compromise caused by a sub-processor (such as Supabase) to the same extent as if Vantic had caused it directly, since your Organization's relationship for the purposes of this Addendum is with Vantic, not with any sub-processor Vantic uses — this does not affect Vantic's own right to seek recovery from that sub-processor separately.

12. Term

This Addendum remains in effect for as long as the Subscription Agreement between your Organization and Vantic remains in effect, and survives its termination to the extent needed to give effect to section 8 (return or deletion of data).

Signatures

Signed on behalf of the parties below.