HEAT

Privacy Policy

Version 2026-11-05 · Effective 5 November 2026 · Nigeria Data Protection Act 2023

This policy explains what personal data the HEAT app and gym collect, why, who we share it with, how long we keep it, and the rights you have under the Nigeria Data Protection Act 2023 (NDPA) and the NDPC General Application and Implementation Directive 2025 (GAID).

1. Who we are
2. What we collect
3. Your fingerprint
4. Opening the door with your phone
5. Why we use your data, and our lawful basis
6. Payments
7. Who we share data with
8. Transfers outside Nigeria
9. How long we keep data
10. Security
11. Your rights
12. Members under 18
13. Data breaches
14. Changes to this policy
15. Contact and complaints

1 Who we are

HEAT is the fitness facility operated at Tahir Guest Palace, 4 Ibrahim Natsugune Road, Giginyu, Kano 700213, Nigeria, by Tahir Guest Palace Limited (RC 303555). HEAT is the **data controller**: it decides why and how your personal data is used.

The HEAT app is built and operated on HEAT's behalf by Nuvira Nigeria Limited (RC 8564977), 26 Tukur Road, Kano. Nuvira is a **data processor**: it handles your data only on HEAT's written instructions and never for its own purposes.

Data protection contact
Anthony Victoria, Receptionist
helpdesk@heatgym.co · +234 805 029 8536 · or the front desk at HEAT reception

Data protection officer
HEAT's Gym Manager, reached the same way

In this policy "we" and "us" mean HEAT. "You" means a member, a coach, or anyone else who uses the app or enters the gym.

2 What we collect

CATEGORY	EXAMPLES	WHERE IT COMES FROM
Identity & contact	Full name, date of birth, gender, phone number, member number; optionally an email address and a profile photo	You, at sign-up or at the front desk
Emergency contact	The name, phone number and relationship of the person you nominate	You. Note that you are giving us someone else's details — please tell them.
Parent or guardian, for a member under 18	Their name, phone number and relationship to the member; when they gave consent and which member of staff took it	The front desk, at registration
Membership	Plan, start and end dates, status, freeze requests and their outcome, free-session balances and how they were spent	Generated by the app
Fingerprint	A mathematical template of the finger you enrol at the door reader — see section 3	The door reader, at enrolment
Access events	Every entry and every refused attempt: time, door, method (fingerprint, phone or front desk), the account used and, for a phone, which phone	The locks and the app
Bookings & training	Classes and coaching sessions booked, attended, cancelled or missed; the coach involved; workouts written for you or by you, and which you marked complete	You and your coach, through the app
Payments	Amount, date, status, reference and description of each payment and each wallet movement; and for a saved card, the brand, last four digits, expiry and the payment provider's token	You and Paystack
Device & technical	Push notification token; your phone's model name, sent when you sign in; the IP address and the browser or app identifier sent with each request to our server, kept in our activity log	Your device
Crash reports	When the app fails: what failed in its code, which addresses on our server it had just called (not what it sent), the app's version, the phone's model and operating system, and a random number for this installation of the app. Never your name, phone number, email or anything you typed.	The app, when it fails
Communications	Support requests and our replies; the notices we sent you and whether they were delivered	You and our staff

Consent records	Which version of each document you accepted, and when; for fingerprint consent, whether you gave it in the app or at the desk, and when you withdrew it	Generated when you accept
CCTV	Footage from the Hotel's cameras covering the gym's entrance, reception, corridors and gym floor. There are no cameras in changing rooms or toilets.	Tahir Guest Palace security systems

We do not collect health or medical information. There is no field anywhere in the app for injuries, conditions, medication, measurements or body composition, and no coach can enter any for you. The health declaration in the Waiver is a statement *you make to us* about your own fitness to train — we record that you made it, not its contents. Anything you volunteer to a coach in conversation is between you and them and is not stored by HEAT.

We also do not run a leaderboard, do not publish members' names or photos to other members, and do not use your data for advertising. The app contains no analytics or advertising software from anyone else, and it does not read your location (section 4 explains the one place Android asks for that permission). It does contain Sentry's crash reporting, which tells us when the app fails and where in its code, and nothing about who was using it.

3 Your fingerprint

A fingerprint is **sensitive personal data** under the NDPA. It is the one thing about you that cannot be reissued if it is ever compromised, so it gets its own section.

- **Where it is held.** Your fingerprint is enrolled on the door's reader, a TTLock product made by Hangzhou Sciener Intelligent Control Technology Co., Ltd. How the reader stores your print, and what TTLock's service keeps about it, is set out in TTLock's own privacy policy, which says data on its platform may be sent to, stored and processed in the United States and possibly other countries. HEAT's own systems never receive your fingerprint.
- **What HEAT holds.** Your consent; the number the reader gave your print, the name it was enrolled under and that it is yours; and each time it opened a door, which counts as a visit. Those entries come to HEAT from the lock's own record at TTLock.
- **Why we use it.** To let you into a gym you have paid for, and to keep out people who have not. The lawful basis is your **express consent**, given in the app under Account, then Ways in, or at the front desk, before any finger is enrolled. We record when you gave it, against which version of the wording, and whether you gave it in the app or to a member of staff.
- **It is optional.** You may refuse, and you may withdraw at any time, in the app or at the desk. Phone unlock and the front desk both work without it, and refusing costs you nothing else — no price difference, no reduced access.
- **How long.** The registration carries your membership's end date, so it stops working by itself when your membership lapses. Ask us and we will delete the enrolment outright, within 30 days.

Enrolment itself happens at the reader, in person. For a member under 18, the consent is given by their parent or guardian at the desk, never in the app.

4 Opening the door with your phone

The app opens a door one way: held to its reader. It works only while your membership is active, and nothing opens unless the app is open on its unlock screen.

- **Held to the reader.** Hold your phone against a door's reader and that door opens over Bluetooth, with a digital key the app holds for you. The phone has to be right against the reader; walking past opens nothing. To give you keys, our server opens an account for you with the lock maker, TTLock, under a random name with nothing about you in it, and sends that account a key to each door. A key lasts a day at most, or to the end of your membership if that is sooner, and is renewed while you use the app.
- **Opened by staff.** If your phone will not open a door, staff can open it from the gym's system: our server asks TTLock's service, and a gateway inside the building opens it. If they open it for you, it is recorded as your visit, with the name of who opened it.
- **Bluetooth and location.** Holding the phone to the reader needs Bluetooth. On Android 11 and older, Android lets an app look for Bluetooth devices only if it holds the location permission, so the app asks for it there. It never reads your location. If we ever add a check that you are at the gym before the door opens, we will update this policy and the app will ask your permission first.
- **One phone at a time.** Your account can be signed in on one phone at a time, because each phone signed in holds your keys. Signing in on another phone signs the first one out, and the key held on it stops working within a day. When you sign in, the app tells us the phone's model name, such as "Samsung SM-A515F", so staff can tell your phones apart.
- We keep the outcome of each unlock — allowed or refused, which door, when, and from which phone.
- Access logs are visible to HEAT management and to authorised Nuvira engineers doing support work. Coaches and other members never see them. You can see your own entry history in the app.

We use those logs to control access, to investigate incidents, to enforce the rule against shared credentials, and to know who was in the building in an emergency. If one membership opens the doors from two phones close together, a member of staff is asked to look into it and may ask you about it. Nothing is refused or decided automatically.

5 Why we use your data, and our lawful basis

The NDPA allows six lawful bases for using personal data: consent, the performance of a contract, a legal obligation, vital interests, the public interest, and legitimate interests. We rely on each of them except the public interest, as the table shows.

PURPOSE	DATA USED	LAWFUL BASIS (NDPA S.25)
Create and run your membership account	Identity, contact, membership	Performance of a contract
Sign you in	Phone number, one-time codes, device	Contract
Let you into the gym	Access events, membership status	Contract; and for the fingerprint specifically, express consent

Keep the premises and its members secure	Access events, CCTV	Legitimate interest in the safety and security of members, staff and the hotel
Take payment and keep financial records	Payments, wallet, membership	Contract; legal obligation (tax and accounting)
Pay coaches	Completed bookings, coach bank details	Contract with the coach; legal obligation
Book classes and coaching, and manage attendance	Bookings, contact, membership	Contract
Deliver your training programme	Workouts, bookings, completions	Contract
Send service messages — receipts, expiry and renewal notices, booking and waitlist alerts, freeze decisions	Contact, device token, membership	Contract
Respond to a medical emergency	Emergency contact, identity, who was in the building	Vital interests
Keep the app working, fix bugs, prevent fraud and abuse	Device & technical, access events	Legitimate interest in a secure, working service
Handle disputes, claims and complaints	Any of the above, as relevant	Legitimate interest in establishing or defending legal claims; legal obligation

Where we rely on legitimate interest we have weighed that interest against your rights and recorded the assessment; ask and we will summarise it. You can object to that processing — see section 11.

We do not send marketing. The app has five kinds of notification — membership, waitlist, bookings, training, and account — and every one of them is a service message about something you asked for or are paying for. There is no promotional category, so there is nothing to opt out of and no marketing consent to give. You can still turn individual categories off in the app; a few, such as membership expiry and payment receipts, we keep on because missing them costs you money or access.

We do not make any decision about you by automated means alone that produces a legal or similarly significant effect. A lapsed membership stops opening the door — that is the contract taking its course, and there is always a person at the desk.

6 Payments

Payments are processed by **Paystack Payments Limited**, licensed by the Central Bank of Nigeria. You top up a wallet held in your account, and your membership and bookings are paid from that balance.

- Card details are entered on Paystack's own secure page. **We never see or store your full card number, CVV or PIN.** If you save a card we keep only Paystack's token plus the brand, last four digits and expiry, so you can recognise it.
- We do not operate direct debits or card mandates. Nothing is taken from your card or your bank unless you start it in the app. If you switch on automatic renewal, it is paid from your wallet balance.
- We keep a full ledger of every wallet movement — what it was for, when, and the balance after — because that is your statement and our accounting record.
- Coaches are paid out to a Nigerian bank account they provide. We hold the payment provider's recipient reference rather than raw bank details, to make and evidence payouts and to meet tax record-keeping obligations.

See Paystack's own privacy policy at paystack.com for how they handle data as a controller in their own right.

7 Who we share data with

RECIPIENT	WHAT THEY GET	WHY
Nuvira Nigeria Ltd	App data, as needed for support	Builds, hosts and maintains the app as our processor
Amazon Web Services, in Ireland	Everything stored, as hosted data	Servers, database and backups
Paystack, a Stripe company; its data is stored in Ireland	Payment and payout information	To take payment and pay coaches
TTLock (Hangzhou Sciener, China)	Lock and credential identifiers, the record that a fingerprint is registered and its validity dates, unlock records; for phone keys, an account in a random name and the keys sent to it with their dates	To operate the door hardware and its credential service
Termii, Nigeria (SMS); Resend, United States (email)	Phone number or email, and the message	To deliver sign-in codes and notices
Expo, United States, which passes notifications to Apple and Google	Push notification token and message	To deliver push notifications to your phone
Sentry (Functional Software, Inc.), in its European region, Germany	Crash reports, as described in section 2	To find and fix faults in the app
Coaches	Your name, photo, your bookings with them, and the workouts they write for you	To deliver the session you booked

Tahir Guest Palace front desk	Your membership, bookings, wallet, and for a member under 18 their guardian's details	To run the gym day to day
Tahir Guest Palace management and security	Access events and incident details, where relevant	Safety and security of the premises
Professional advisers, insurers, auditors	Only what is necessary	Legal advice, claims, audit
Law enforcement, regulators, courts	Only what is legally required	To comply with the law or a valid order

We do not sell your personal data, and we do not share it with advertisers or data brokers. Every processor is bound by a written contract requiring confidentiality, security measures and processing only on our instructions, and giving your data the same protection this policy does.

8 Transfers outside Nigeria

Some providers store or process data outside Nigeria:

- **Ireland:** our servers, database and backups (Amazon Web Services), and Paystack's payment records;
- **Germany:** crash reports, held by Sentry, a United States company, in its European region;
- **the United States:** email delivery (Resend) and push notifications (Expo);
- **TTLock**, the lock maker, is a Chinese company. Its published privacy policy says data on its platform, which includes the record of your door credentials, may be sent to, stored and processed in the United States and possibly other countries.

We make a transfer only where Part VIII of the NDPA allows it: an adequacy determination by the NDPC, contractual safeguards binding the recipient to an adequate standard of protection, or another lawful ground under section 43. Where a country has no adequacy determination from the NDPC, we rely on your consent, which you give by accepting this policy, having been told that your data there is not protected by Nigerian law in the same way. We record the basis for each transfer; ask us and we will tell you which applies.

9 How long we keep data

DATA	RETENTION PERIOD
Account and membership records	While your membership is active, then 24 months; or until you delete your account, when what identifies you is erased within 30 days
Fingerprint enrolment	Until your membership ends or you withdraw consent, then deleted within 30 days
Access and unlock logs	12 months, unless held longer for a specific incident
Booking, attendance and workout history	24 months

Payment, wallet ledger and payout records	6 years, to meet tax and accounting obligations
Waiver and consent records	6 years after membership ends, as evidence of the agreement
Crash reports	90 days at most, then deleted by Sentry
Support messages	24 months
CCTV footage	7 days, unless retained for an incident

After these periods we delete the data or irreversibly anonymise it. Anonymous, aggregated statistics — how busy the gym is by hour, for instance — may be kept indefinitely, because they can no longer identify anyone.

10 Security

- Data is encrypted in transit (TLS) and at rest.
- Sign-in is by one-time code to your registered phone number. We store no member passwords at all; staff passwords are stored only as salted hashes.
- Access to member data is role-based — staff and engineers get only what their job needs, and administrative actions are written to an audit log that records who did what and when.
- Door credentials carry your membership's end date, and a phone key lasts a day at most, so they expire on their own rather than depending on somebody remembering to revoke them.
- We never store card numbers, CVVs, PINs or bank login credentials.
- Backups are encrypted and access to them is restricted.
- Staff and coaches are bound by confidentiality obligations and are trained on data protection.

No system is perfectly secure. Keep your phone locked, and tell us at helpdesk@heatgym.co immediately if it is lost or stolen, so we can end every session it holds.

11 Your rights

Under the NDPA you have the right to:

- be told how your data is used — this policy;
- access a copy of the personal data we hold about you;
- correct data that is inaccurate or incomplete;
- delete your account and your data where we no longer have a lawful reason to keep it — in the app under Account, then Profile, or as described at heatgym.co/delete-account. Your account closes at once and what identifies you is erased within 30 days;
- restrict processing while a dispute about accuracy or lawfulness is resolved;
- object to processing based on legitimate interest;
- withdraw consent at any time, without penalty, where we rely on consent — including your fingerprint. Withdrawal does not affect processing already carried out;

- receive your data in a structured, commonly used, machine-readable format, or have it sent to another controller where technically feasible;
- not be subject to a decision based solely on automated processing that significantly affects you;
- complain to the Nigeria Data Protection Commission.

To exercise any of these, email helpdesk@heatgym.co or ask at the front desk. We may ask you to confirm your identity. We respond without undue delay and in any case within 30 days; if a request is complex we may extend once and will tell you why. Exercising your rights is free, unless a request is manifestly unfounded or excessive.

Some data we must keep even if you ask us to delete it — payment records we are required to retain for tax, and waiver and consent records we need if a claim is ever brought. We will tell you when that applies and why.

12 Members under 18

Under the NDPA anyone under 18 is a child. The app's own sign-up is for members aged 18 and over: it refuses a younger date of birth and sends the person to the front desk. Members aged 16 and 17 join at the front desk, where:

- a parent or legal guardian signs the Membership Terms and the Waiver and consents to the processing of the member's data;
- a member of staff sights the guardian's identification, and records the guardian's name, phone number and relationship, and that they took the consent and when. We do not copy or store the identification document;
- fingerprint consent for the member, if wanted, is given by the guardian at the desk;
- a guardian may access, correct or delete the member's data, and may withdraw consent at any time, which ends the membership.

Once registered, the member may use the app. We do not admit members under 16.

13 Data breaches

If a personal data breach occurs we will notify the Nigeria Data Protection Commission within **72 hours** of becoming aware of it, where the breach is likely to result in a risk to your rights and freedoms. If your data is involved we will also tell you directly and without delay, in plain language — what happened, what data was involved, what we are doing, what you should do, and who to contact. We keep a record of every breach.

14 Changes to this policy

We may update this policy as the app, the law or our providers change. The version and effective date at the top always show the current one. For a change that materially affects your rights we will notify you in the app at least 14 days before it takes effect, and the app asks you to accept the new version before you carry on using it.

15 Contact and complaints

HEAT — data protection contact
Anthony Victoria, Receptionist
Tahir Guest Palace, 4 Ibrahim Natsugune Road, Giginyu, Kano 700213
helpdesk@heatgym.co · +234 805 029 8536

Data protection officer
HEAT's Gym Manager, at the same address

App operator
Nuvira Nigeria Limited, 26 Tukur Road, Kano · issafares@nurvina.io

If you are not satisfied with our response you can complain to the **Nigeria Data Protection Commission (NDPC)**, 1919 Cadastral Zone C06, Mbora District, opposite Efab City Estate, Life Camp, Abuja — info@ndpc.gov.ng, +234 916 061 5551, ndpc.gov.ng. You may also seek a remedy in court.

HEAT · operated at Tahir Guest Palace, Kano · app by Nuvira Nigeria Limited
Privacy Policy, version 2026-11-05 — effective 5 November 2026