Draft. Final wording is being reviewed by our Nigerian lawyer and data protection officer.

Privacy Policy

Version 1.0. Effective from 7 October 2026. taxaudit.ng

In plain English

- We collect what we need to run TaxAudit and nothing for advertising.
- Your business records are processed on your instructions: we never sell them and they are never used to train AI models.
- Analytics only run if you agree.
- Our main servers are in the European Union.
- You can see, correct, export or delete your data, and ask a person to review anything our AI suggested.

This summary helps you read the document; it doesn't replace it.

1. Who we are and how to contact us

- **Rivium Analytics Ltd** (RC 8927769), 1 Udo Umana Street, Uyo, Akwa Ibom State, Nigeria, provides TaxAudit and TaxAuditPro.
- **Controller** for account, billing and website data. For the business records you put into TaxAudit, the business (or its accounting firm) is the controller and we are its **processor**, acting on its instructions under our Data Processing Agreement.
- **Data Protection Officer:** dpo@taxaudit.ng. Security issues: security@taxaudit.ng.

2. What we collect

- **Account**: What: Name, email address, password (stored only as a secure hash, never readable), account type; Where it comes from: You, at sign-up
- **Sign-in security**: What: Two-step verification data (authenticator app or passkey details, recovery codes), records of sign-ins, failed sign-ins and security changes; Where it comes from: Your use of TaxAudit
- **Devices**: What: A one-way fingerprint of your browser or app (we keep a hash, not the browser details themselves), a short readable description such as "Chrome on Windows", and a hashed form of your IP address; Where it comes from: Each sign-in, to warn you about sign-ins from new devices
- **Phone number *(optional; not in use yet)***: What: Mobile number, and whether it's verified; Where it comes from: Only if you add one, once we switch on SMS codes [see section 4 note]
- **Business records**: What: Business details (name, CAC number, Tax ID, address, registrations), documents and figures you upload or enter; Where it comes from: You or your accountant
- **Activity and history**: What: A record of changes to your business's data (who, when, what changed, through which channel); Where it comes from: Kept automatically for audit evidence
- **Usage analytics *(only with consent)***: What: Pages and features used, approximate location derived from your IP address (country or region); Where it comes from: Our analytics tool, only if you accept analytics cookies
- **Payments**: What: Plan, invoices and payment references. **Card details never reach us**: they go straight to our payment provider; Where it comes from: Paystack or Flutterwave

- **Support**: What: Messages and attachments you send us; Where it comes from: Help and support
- **Contact form**: What: Your name, email address, topic, business or practice name (optional) and message (the message is **encrypted** in our database), and a hashed form of your IP address to stop abuse. Demo requests (pro.taxaudit.ng) also ask for your practice's name, how many clients it serves and when suits you; Where it comes from: You, through the contact or demo form on our websites
- **Product updates**: What: Which "What's new" notes you've read, and when (so we don't show them as new again); Where it comes from: Your use of TaxAudit
- **Your choices about our policies and cookies**: What: Which versions of the Terms of Service and Privacy Policy you accepted and when; each cookie choice (analytics yes or no) with the Cookie Policy version, a random visitor ID kept in the ta_consent cookie, and a hashed form of your IP address; Where it comes from: Sign-up, the "We've updated our Terms" page, and the cookie banner or settings

We do **not** collect your BVN. Tax IDs (and NINs if we ever need them) are **encrypted** in our database.

3. Why we use it, and our lawful bases (NDPA 2023)

- **Providing TaxAudit: your account, your records, statements and checks**: Lawful basis: Contract
- **Keeping accounts secure: two-step verification, sign-in alerts, blocking repeated wrong passwords, checking passwords against known breaches**: Lawful basis: Legitimate interests (security) and contract
- **Audit trail and history of changes**: Lawful basis: Legal obligation (tax record-keeping) and legitimate interests (evidence)
- **Product analytics**: Lawful basis: Consent (cookie choice), which you can withdraw at any time
- **Service emails (verification codes, security alerts, receipts)**: Lawful basis: Contract and legitimate interests
- **Marketing emails and newsletters**: Lawful basis: Consent (double opt-in), withdrawable at any time
- **Answering messages sent through our contact form, and keeping the form free of spam and abuse**: Lawful basis: Legitimate interests (replying to you; protecting the form), and steps you ask for before a contract (such as a demo)
- **Keeping a record of which terms you accepted and which cookies you allowed, so we can show what you agreed to**: Lawful basis: Contract (terms) and legal obligation (proving consent under the NDPA)
- **Meeting legal and regulatory duties**: Lawful basis: Legal obligation

4. AI processing

- Some features use AI from **Anthropic** (Claude), for example reading uploaded documents or explaining a failed check. Only the data the task needs is sent. Email addresses, phone numbers, bank account numbers (we keep the last four digits), NIN/BVN-style ID numbers and Tax IDs are **masked before anything is sent**, unless a task genuinely needs one.
- For each AI request we keep a **usage record** (which feature, when, for which business, how much it cost and whether it worked), **not the text of your question or the AI's answer**.
- When the AI looks something up to help you (for example your business profile), it acts **as you**: it sees only the business you're working in and only what you're allowed to see. What it looks up is

masked the same way before it's sent.
- **A person approves every figure.** The AI suggests; it cannot finalise statements, filings or approvals. When the AI suggests a change, we keep the **suggestion** (what it would change, the values at the time, its reason, how confident it was and its sources, and who it was working for) and the **decision** (who accepted, edited or rejected it, and when). This is part of your business's records: it shows who decided each figure. Nothing changes until a person with the right role accepts; undecided suggestions expire after 30 days.
- Your data is **not used to train AI models**.
- You can ask for **a person to review** any AI-assisted outcome (section 8).
- *Note on SMS:* SMS one-time codes are built but **switched off**. If we switch them on, this section and section 5 will add the SMS provider before it's used.

5. Who we share it with

Only these service providers ("sub-processors"), under contract, and authorities where the law requires:

- **Neon**: What for: Database (PostgreSQL); Where: EU (AWS Frankfurt)
- **Render**: What for: Running the application; Where: EU (Frankfurt, Germany)
- **Cloudflare**: What for: Website delivery, security, file storage and encrypted backups (R2), and the spam check on our contact form (Turnstile); Where: Global network; stored files and backups in the EU
- **Anthropic**: What for: AI features; Where: United States
- **PostHog**: What for: **Product analytics (with consent) and feature rollouts**; Where: **EU cloud**
- **Sentry**: What for: Error tracking: technical error details only; personal data (emails, numbers, addresses, cookies, form contents) removed before sending; Where: EU (Germany)
- **Brevo**: What for: Sending emails (sign-up and sign-in codes, account notices, contact form messages to our team); Where: EU (Frankfurt, Germany)
- **Hostinger**: What for: Our team's email inboxes (hello@, support@, dpo@, security@taxaudit.ng): messages you send us and our replies; Where: being confirmed
- **Google (Gmail)**: What for: Temporarily, our team receives contact form messages in a Gmail inbox; Where: United States
- **Paystack, Flutterwave**: What for: Payments; Where: Nigeria
- **Have I Been Pwned**: What for: Checking whether a password appears in known breaches; Where: See note below

Cloudflare Turnstile (contact form spam check): when you open our Contact page, Cloudflare's check runs in a small Cloudflare frame and looks at signals from your browser to tell people from bots, without a puzzle in most cases. It's a security measure, so it doesn't need a cookie choice. Our server sends the check's result token and your IP address to Cloudflare once, to confirm the check.

PostHog, in detail (verified 2026-10-05):

- Analytics events are only collected **if you accept analytics cookies**.
- **Essential cookies** keep you signed in, protect forms against forgery and remember your choices. One remembers your **appearance** (light or dark; ta_theme, one year, set only if you choose) and one your **cookie choice** (ta_consent, 6 months). They're needed for TaxAudit to work as you asked and are never used for tracking. Every cookie is listed in our Cookie Policy.

- Our fonts and scripts are served from our own site, so loading a TaxAudit page doesn't contact Google or other font or script providers.
- **Your IP address is not stored.** PostHog uses it briefly to work out an approximate location (such as the country) and to detect bots, then discards it.
- PostHog's own **AI features and AI training are switched off** for our account, so our data isn't sent to third-party AI services or used to train PostHog's AI.
- When we check whether a feature is switched on for you (a "feature flag"), the check happens **on our own servers**; no information about you is sent to PostHog for that (our flags connection is configured so it cannot send any events).

Password breach check, in detail: when you choose a password, we turn it into a one-way code and send only the **first 5 characters** of that code to Have I Been Pwned. Your password, and even its full code, never leave our servers, and the service can't tell which password you chose.

The full, current list (with any changes announced in advance) is on our Sub-processors page.

6. Transfers outside Nigeria

Our main hosting is in the **European Union**; AI processing is in the **United States**. We rely on the safeguards the NDPA requires for these transfers (contracts with each provider).

7. How long we keep it

- **Business tax records and documents**: Kept for: The statutory record-keeping period, even after you leave, unless the law allows deletion earlier
- **Audit trail and change history**: Kept for: As long as the records they relate to (they are evidence)
- **Account and billing data**: Kept for: While your account is open, then the period required for our own tax records
- **Sign-in device records**: Kept for:
- **Signed-in devices list (app or browser name, shortened IP address, sign-in time)**: Kept for: While that device stays signed in (until you sign out, sign it out from another device, or the session expires)
- **Support conversations, data requests, concern reports**: Kept for: 3 years after closing
- **Messages sent through the contact form**: Kept for: 24 months, then deleted automatically
- **Which What's new notes you've read**: Kept for: While your account is open
- **Records of which policy versions you accepted, and of your cookie choices**: Kept for: As long as we need to show what you agreed to, then deleted
- **AI suggestions and the decisions on them**: Kept for: As long as the records they relate to (they are evidence of who decided)
- **Error reports (technical details, personal data removed)**: Kept for: 30 days
- **Analytics**: Kept for: 12 months
- **Marketing contacts**: Kept for: Until you unsubscribe, or 24 months without activity
- **Backups of our database (encrypted; only we hold the key)**: Kept for: 30 days, rolling
- **Unfinished uploads from the app (the parts of a file received so far, its name, size and fingerprint)**: Kept for: The parts: until the file is complete, or 15 days if the upload is never finished. The upload's record (name, size, who sent it, when) as long as the business's records
- **Background task records (which account asked, the business and record IDs, a hashed IP; no document contents)**: Kept for: 30 days after the task finishes; 90 days if it failed, for

investigation

8. Your rights

You can ask to **access**, **correct**, **delete** or **export** your data, **object** to some uses, **withdraw consent**, **restrict** processing, and ask for **a person to review** an AI-assisted outcome. Use "Request your data" (taxaudit.ng/data-request) or email dpo@taxaudit.ng. Where the law requires us to keep tax records, we tell you what we keep, why and for how long. If an accounting firm manages your business's records, we pass your request to them and help them respond.

9. Security

- **Data is encrypted in transit:** HTTPS only (TLS 1.2 or newer) between your device and our network, and between our network and our servers, with each side's certificate checked. Tax IDs (and NINs if collected) are also encrypted in our database.
- **Each business's data is isolated** by the database itself, so one customer can never see another's records.
- **Two-step verification** is available to everyone and required for our staff. The secrets behind it (your authenticator-app key and recovery codes) are **encrypted** in our database.
- You get an email when your account signs in from a new device. Repeated wrong passwords temporarily lock sign-in.
- You can see **your signed-in devices** (website and app) and sign any of them out. For each we keep the app or browser name, a **shortened IP address** (the network, not your exact address) and when it signed in, only while it stays signed in. The mobile app keeps its sign-in token in your phone's secure storage.
- Before sensitive changes (email, password, phone, two-step settings) we ask for a code sent to your email.
- **Our staff can't see your business's records** unless you grant time-limited support access, with a reason; every access is logged and visible to you.
- Every change to business records is kept in a history that can't be altered.
- To protect the service from abuse, we use your device's **IP address for about a minute** to limit how many requests can be made from it. It isn't linked to your account or kept afterwards.
- **Your documents are stored privately** in Cloudflare R2 in the EU. They can only be opened through a link that works for a few minutes, created after we check you may see the file. Each file is fingerprinted when stored, so we can prove it hasn't changed. The app sends files in small parts so a weak signal doesn't lose them; the parts are kept privately in the same storage and deleted once the file is complete (or after 15 days if it never is). A file your business already has isn't sent again.
- Our website's pages and images are managed by our staff in a content system inside the staff area, behind the same staff sign-in and two-step verification. Website images are public and kept apart from your documents; they never contain customer data. It loads no profile pictures from outside services (such as Gravatar) and doesn't contact its maker for updates.
- **Backups:** our database is backed up every night, encrypted with a key that only we hold (our hosting and storage providers can't read it), stored privately in the EU and kept for 30 days. We test that backups restore.
- **Errors** are reported to our error-tracking provider (Sentry, EU) with personal data removed first: no names, emails, numbers, addresses, cookies or form contents.

More on our Security page (our Security page).

10. Complaints

Contact our DPO first (dpo@taxaudit.ng). You can also complain to the **Nigeria Data Protection Commission (NDPC)**.

11. Changes to this policy

We publish every version with its date and what changed. For important changes we notify you in advance, and where needed ask you to accept again.