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

Privacy Policy

Version 1.1. 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.
- TaxAudit's AI works with your records only if you allow it.
- 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. 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.
- The **TaxAudit apps** on Google Play and the App Store are published for us by **Rivium Analytics LLC**, 4539 N 22nd St, Phoenix, AZ 85016-4639, USA. Rivium Analytics Ltd provides the service and is responsible for your data as this policy describes.
- **Data Protection Officer:** dpo@taxaudit.ng. Security issues: security@taxaudit.ng.

2. 2. What we collect

- **Account**: Name, email address, password (stored only as a secure hash, never readable), account type. *Where it comes from:* You, at sign-up (on the website or in the app).
- **Profile photo** *(optional)*: A photo of you, if you add one in the app's Profile: we keep only a new 256 x 256 copy (nothing else from the original, such as the camera, the date or where it was taken). Shown to you in the app and the website's menu; deleted when you remove it or your account is deleted. *Where it comes from:* You, in the app.
- **Partner code** *(optional)*: The code of a partner who sent you to TaxAudit, if you came through their link or typed it in. *Where it comes from:* You, at sign-up (filled in for you from a partner's link; no cookie is used).
- **Sign in with Google** *(optional)*: If you choose "Continue with Google": your Google account's email address (and that Google has verified it), your name, and Google's ID number for your account, so the same Google account signs you in next time. We don't receive your Google password and don't keep any access to your Google data (no Google tokens are stored). *Where it comes from:* Google, when you choose it at sign-up or sign-in.

- **Sign-in security**: 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**: 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" or "the TaxAudit app on iPhone", and a hashed form of your IP address. The app also sends its version and your phone's system (iPhone or Android, and its version) with each request, so we can ask you to update an app that's too old; we don't keep them apart from that description. *Where it comes from:* Each sign-in, to warn you about sign-ins from new devices; each request from the app.
- **Phone number** *(optional; not in use yet)*: Mobile number, and whether it's verified. *Where it comes from:* Only if you add one, once we switch on SMS codes (see the note in section 4).
- **Business records**: Business details (name, CAC number, Tax ID, address, registrations), documents and figures you upload or enter. *Where it comes from:* You or your accountant.
- **Accounting software** *(if you connect QuickBooks Online or Xero)*: The connected company's name and ID in that software, the trial balances you bring in (each account's name, code and balances), and the connection's sign-in tokens, **encrypted** and deleted as soon as you disconnect it or close the business. TaxAudit only reads, when you choose to bring a trial balance in. *Where it comes from:* Your accounting software, when you connect it. *Why:* Preparing your statements from your own books; you decide when to bring a trial balance in.
- **Employees' pay** *(if you import a payroll register)*: Each employee's name, designation, email address, mobile number and Tax ID (the last three **encrypted**), annual rent paid (for rent relief), and each month's gross pay, pension, NHF, NHIS, NSITF, life assurance and PAYE; the register file you uploaded; how your files' columns are laid out (headings and what each holds); when the AI is on, the headings and masked sample values are sent to our AI provider to suggest the columns (names, account numbers, phone numbers, emails and Tax IDs never are). Bank account numbers in the file are read for a check and never kept. *Where it comes from:* You, from your payroll. *Why:* Preparing your PAYE returns (Form H1, monthly PAYE schedules) and checking them against your records; you decide what to import, and TaxAudit processes it for you.
- **Your customers and suppliers** *(if you add them)*: Each name, whether a customer or supplier, company or individual, resident or not, address, State and Local Government, and its Tax ID, RC number or NIN (**encrypted**); each sale or payment listed under a monthly total (date, description, invoice number, amount, VAT category, WHT deducted by you or by the customer, VAT withheld) and customers' WHT credit notes you upload; the supplier or customer named on a year-end unpaid bill or money owed (with what it was for, the amount and the bill or invoice you attach); any register or list file you uploaded. *Where it comes from:* You, typed or imported from your sales or purchase records; the AI's reading of a receipt you attached, offered for you to confirm. If you ask the AI to look for a year's unpaid bills, the money-out payments entered for the first two months after the year (who was paid, which may be a person such as a market seller on a payment voucher, the date, row, amount, description and what the AI read on an attached bill) and the business's name and type are sent to our AI provider (phone numbers masked; not used for training); its suggestions are kept for you to add or dismiss. *Why:* Preparing NRS's VAT and WHT schedules, your WHT payable and your statements; you decide what to add, and TaxAudit processes it for you.
- **People you pay without a receipt** *(if you raise payment vouchers)*: The name of the person paid (for example a market seller), their phone number if you add it (**encrypted**) and their market or place; what was bought, quantities, prices and the amount; the date, how it was paid, why there was no receipt and what it was for; who in your business raised and approved the voucher, and when; if you upload them, a signed copy of the voucher (which may show the payee's signature or

thumbprint) and photos of the goods, the stall or a transfer. *Where it comes from:* You, typed when you raise the voucher, and files you upload. If you ask the AI to fill a voucher in, your description (which may name the person paid and their market) is sent to our AI provider, with phone numbers masked, and the AI's filled-in form is offered for you to check (not used for training). *Why:* Proving your business's costs for tax (your records must hold sufficient information on every transaction); you decide what to add, and TaxAudit processes it for you.

- **Activity and history**: 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)*: 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**: 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**: Messages and attachments you send us. *Where it comes from:* Help and support.
- **Business set-up and team**: How your business is registered, VAT and withholding tax, employee count, yearly sales band and financial year; your CAC certificate (a file you upload, or in the mobile app a photo you take with your phone's camera or a file you choose from your phone; stored privately; read by our AI provider with your confirmation when the AI guide is on). In the app, the camera is used only when you choose to take that photo. For team invitations: the invited person's email address, role, who invited them and when, and for an accounting practice which of its clients they'll work on. When they join, the team's owners and the person who invited them are emailed their name, email address and role. *Where it comes from:* You, during set-up (on the website or in the app) and in Settings.
- **Pre-audit check and evidence packs**: Each check you run: who ran it and when, what it found (which may name the business, its registrations and figures such as tax deducted from staff pay) and the estimated amounts at risk; the year's payment vouchers, listed with who was paid (shown to your team, not sent to the AI); the index narrative and who approved it; for every evidence pack downloaded, who downloaded it, when, and the name, size and fingerprint (SHA-256) of each file in it (we don't keep a copy of the pack itself). When the AI auditor is switched on, the findings, the business's name and type and the pack's contents list are sent to our AI provider to be worded as an auditor would (emails and phone numbers masked; not used for training). *Where it comes from:* Your use of the pre-audit check.
- **The AI assistant** *(when switched on)*: Your questions to TaxAudit AI and its answers, the pages and rules it used, kept with your account for the business you asked about (only you see your conversations); what it looked up in your records is sent to our AI provider to answer (emails and phone numbers masked; not used for training). Your ■/■ ratings of AI answers and the reason you chose. *Where it comes from:* You, in the AI panel.
- **Letters from tax authorities**: Letters and demand notices you upload (which may name the business's owners, directors or staff and its tax figures), what they ask for, your reply and who wrote, sent and approved it, and for each reply pack exported who, when and each file's name, size and fingerprint (we don't keep a copy of the pack). When the AI is switched on, the letter itself and the list of requests with what you hold are sent to our AI provider to read it and draft the reply (not used for training). *Where it comes from:* You, when you upload a letter.
- **Feedback you send**: Your message (**encrypted**) and its kind; only if you tick the box, the page you were on, your browser and screen size and a screenshot. Deleted after 24 months. *Where it comes from:* You, with "Give feedback".

- **Support tickets**: What you write in a ticket and our replies (**encrypted** in our database), files you attach (stored privately), the category, urgency and business it's about, the page you were on, your app or browser version, your rating of our help if you give one, and, if you allow it, a record of each time our support staff open your business's records (who, when, until when). Our team's internal notes on a ticket are not shown to you but are part of your data if you ask for it. To help our team answer faster, the text of your ticket is sent to our AI provider, with personal details such as emails and phone numbers masked, for a suggested category, urgency and draft reply; our staff check and edit every reply before it's sent, and the suggestions are kept **encrypted** with the ticket When the AI is switched on, the subjects of recently solved tickets and our replies (not what you wrote; emails and phone numbers masked) may also be sent to our AI provider to draft help-centre articles about common questions; our staff edit every article, and no customer's name, business or figures are copied into it. *Where it comes from:* You, when you open or answer a ticket in the app.
- **Help centre**: The words you search for and how many articles matched (never who searched), whether you found an article helpful (yes or no, anonymous), and how many times each article is read per day (a count only). If you're signed in and ask for a quick answer, your question is sent to our AI provider with personal details such as emails and phone numbers masked; we record that an answer was given, which articles it cited and whether you found it helpful, not the question or who asked. *Where it comes from:* Your use of the help centre.
- **Contact form**: 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. Our replies to you (sent by email from support@taxaudit.ng) and our team's internal notes are kept with your message, also **encrypted**. If you have a TaxAudit account, we may turn your message into a support ticket and tell you by email. *Where it comes from:* You, through the contact or demo form on our websites.
- **Data requests and concern reports**: For a data request: your name, email address, what you asked for and any details you add (**encrypted**), when you confirmed it's you, our questions and answers, what we did and what the law requires us to keep, and whether we passed it to the accounting firm that manages your records. For a concern report: its category, what you tell us (**encrypted**), files you attach (stored privately), and your email for updates, unless you report anonymously, in which case we keep no email or account link and send no emails. For both, a hashed form of your IP address to stop abuse and our team's internal notes. Deleted 3 years after the case is closed. *Where it comes from:* You, through "Request your data" (taxaudit.ng/data-request) or "Report a concern" (taxaudit.ng/report).
- **People invited to our staff area** *(for example an external auditor)*: Name, email address, organisation, engagement reference, why access is needed, which areas they can view or change, the end date, who invited them, and each sign-in and change they make. *Where it comes from:* Our team, when they invite you.
- **Product updates**: 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**: 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. 3. Why we use it, and our lawful bases (NDPA 2023)

- **Providing TaxAudit: your account, your records, statements and checks:** Contract.
- **Keeping accounts secure: two-step verification, sign-in alerts, blocking repeated wrong passwords, checking passwords against known breaches:** Legitimate interests (security) and contract.
- **Audit trail and history of changes:** Legal obligation (tax record-keeping) and legitimate interests (evidence).
- **Product analytics:** Consent (cookie choice), which you can withdraw at any time.
- **Service emails (verification codes, security alerts, receipts):** Contract and legitimate interests.
- **Marketing emails and newsletters:** Consent (double opt-in), withdrawable at any time.
- **Paying the partner who referred you: telling our partner portal you signed up with their code, and about your plan payments, refunds and stopping paying:** Legitimate interests (paying partners for the customers they bring).
- **Answering messages sent through our contact form, and keeping the form free of spam and abuse:** 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:** Contract (terms) and legal obligation (NDPA: proving consent).
- **Meeting legal and regulatory duties:** Legal obligation.

4. 4. AI processing

- **You decide whether TaxAudit's AI works with your records.** We ask once, in the app and on the website ("TaxAudit's AI and your records": what it does, that it's sent to Anthropic, and that it's never used for training), and nothing is sent to the AI for you until you allow it. You can change your answer any time (in the app: More → Profile and security; on the website: Settings → Data and privacy). If you haven't allowed it, or turn it off, everything still works by hand: your uploads are kept "Not read" and read once you allow it, and support answers your tickets without the AI's help. We keep your answer, the wording you answered and when, in your account's history.
- 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**. Usage records are kept with your business's records; those not tied to a business (such as the website's guide) are deleted after 12 months.
- Each new file the AI reads is **counted against your plan's document reads** for the month: we keep which account and business it was for, which file (by its ID, not its content), the month, and whether it was one of the plan's reads or an extra read that used AI credits. It's part of your billing records, kept with them.
- 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. One exception: a receipt, invoice or POS report the AI reads with confidence is filed on its month's row in your monthly records, marked "Filed by the AI" until a person checks it, and a total nobody has typed shows what its receipts add up to while the month is being entered. The AI never changes a figure a person typed, and never submits or approves a month.
- 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. 5. Who we share it with

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

- **Neon**: Database (PostgreSQL) (EU (AWS Frankfurt)).
- **Render**: Running the application (EU (Frankfurt, Germany)).
- **Cloudflare**: Website delivery, security, file storage and encrypted backups (R2), and the spam check on our contact form (Turnstile) (Global network; stored files and backups in the EU).
- **Anthropic**: AI features (United States).
- **Paystack**: Card payments and subscriptions (when payments are switched on) (Nigeria).
- **PostHog**: **Product analytics (with consent) and feature rollouts** (**EU cloud**).
- **Sentry**: Error tracking: technical error details only; personal data (emails, numbers, addresses, cookies, form contents) removed before sending (EU (Germany)).
- **Brevo**: Sending emails (sign-up and sign-in codes, account notices, contact form messages to our team) (EU (Frankfurt, Germany)).
- **Expo (650 Industries)**: Delivering the TaxAudit app's notifications to your phone through Apple's and Google's push services: the phone's push address and the notification's words (what happened and for which business) (United States).
- **Google (Firebase Cloud Messaging)**: Delivering the TaxAudit app's notifications to Android phones: the phone's Firebase installation ID and push address, and the notification's words. No analytics: Google Analytics is off in our Firebase project (United States).
- **Hostinger**: Our team's email inboxes (hello@, support@, dpo@, security@taxaudit.ng): messages you send us and our replies (Hostinger's data centres).
- **Google (Gmail)**: For now, our team receives contact form messages in a Gmail inbox (United States).
- **Google (sign-in)**: Only if you choose "Continue with Google": confirms who you are and sends us your email address and name. Google sets its own cookies on its own pages (United States (Google's own privacy policy applies on Google's pages)).
- **Paystack, Flutterwave**: Payments (Nigeria).
- **Have I Been Pwned**: Checking whether a password appears in known breaches (See note below).
- **Rivium Partners, our partner portal (Rivium Analytics Ltd), hosted on Railway with its database at Neon**: Paying the partner who referred you, only if you signed up with a partner's code: see below (United States).

A partner who referred you, only if you signed up with a partner's code: our partner portal receives the code, a shortened form of your email address (like ad•••@gmail.com), a one-way fingerprint of it (so a

partner can't earn on their own business; it can't be turned back into your address), your account's ID, and for each plan payment its amount before VAT, date and reference, plus any refund and when you stop paying. The partner sees the shortened address and whether you're paying, never your records, invoices or anything you put into TaxAudit.

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. Cloudflare says Turnstile doesn't use the data for advertising. Our server sends the check's result token and your IP address to Cloudflare once, to confirm the check.

PostHog, in detail:

- 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** (dark, or the same as your device; ta_theme, one year, set only if you choose; light needs none) and one your **cookie choice** (ta_consent, 6 months). One more, ta_kept (5 minutes, a random number only), tells your browser a form you sent has arrived. They're needed for TaxAudit to work as you asked and are never used for tracking. Every cookie is listed in the Cookie Policy, from a list the site is tested against.
- **What you type stays on your device until it's saved.** While you fill in a form, your browser keeps a copy of what you've typed in that tab's own storage, so a dropped connection or a reload doesn't lose it. The copy never leaves your device, is removed once the form is saved or you sign out, and is gone when you close the tab. Passwords, security codes, card details and files are never kept.
- 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.

Payment voucher check codes. A payment voucher printed from TaxAudit carries a check code. Anyone who has the code (for example your auditor, from the paper copy) can confirm the voucher at taxaudit.ng/v/: they see only your business's name and the voucher's number, date paid, amount and status, never who was paid or what was bought. Lookups are limited per visitor so codes can't be guessed.

6. 6. Transfers outside Nigeria

Our main hosting is in the **European Union**; AI processing is in the **United States**, and so is the partner portal's database (section 5), for customers a partner referred. We rely on the safeguards the NDPA requires for these transfers (contracts with each provider).

7. 7. How long we keep it

- **Business tax records and documents**: While your business uses TaxAudit. If you close the business (Settings → Profile), each financial year is kept until 6 years after its year of assessment, as the tax law requires (Nigeria Tax Administration Act 2025, section 31(5)), then deleted with its documents, their files and what our AI did with them; until then you can download everything and reopen it. We email the owner 30 days before the first year is deleted. The year's closing balances (what the business had and owed, with no personal data) are kept as the next year's opening balances. The business's profile, team, customers and suppliers, and employees are deleted with its last year. Kept longer only while a legal hold applies (for example a tax audit, a dispute or a court order).
- **Audit trail (who changed what, and when)**: Changes to records, statements, returns, payroll and documents: 6 years. Sign-ins, sessions, security and settings: 2 years. Then deleted.
- **Account and billing data**: While your account is open, then the period required for our own tax records.
- **Sign-in device records**: While your account is open.
- **Signed-in devices list (app or browser name, shortened IP address, sign-in time)**: While that device stays signed in (until you sign out, sign it out from another device, or the session expires).
- **Places you've signed in from (city and country only, worked out by Cloudflare; no address is kept), used to warn you about a sign-in from somewhere new**: While your account is open.
- **Support conversations and tickets with their messages and files, data requests, concern reports**: 3 years after closing, then deleted automatically.
- **Messages sent through the contact form, with our replies and notes**: 3 years, then deleted automatically; messages we mark as spam are deleted 30 days later.
- **Help centre searches (the words only, never who searched)**: 90 days, then deleted automatically.
- **"Was this helpful?" answers and daily article read counts**: Kept as anonymous totals.
- **Which What's new notes you've read**: While your account is open.
- **Records of which Terms and Privacy Policy versions you accepted**: While your account is open, and afterwards as long as the law needs them as proof.
- **Records of your cookie choices**: As long as we need them to prove your choice.
- **Your conversations with the AI assistant, and your ratings of AI answers**: While your account is open.
- **Letters from tax authorities, their requests and replies, and the record of each reply pack exported**: As long as the business records they relate to.
- **Pre-audit checks, their findings and the record of each evidence pack downloaded**: As long as the business records they were made from.
- **AI suggestions and the decisions on them**: As long as the records they relate to (they are evidence of who decided).
- **Error reports (technical details, personal data removed)**: 30 days.
- **"Download everything" files (a ZIP of a business's records you asked for)**: 7 days, then deleted automatically.
- **Analytics**: 12 months.
- **Marketing contacts**: Until you unsubscribe, or 24 months without activity.

- **Backups of our database (encrypted; only we hold the key)**: 30 days, rolling.
- **Unfinished uploads from the app (the parts of a file received so far, its name, size and fingerprint)**: 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)**: 30 days after the task finishes; 90 days if it failed, for investigation.

8. 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.

We reply within **30 days** of confirming it's you. You confirm it's you through a link we email to the address on your account; if you don't confirm within 10 days the request is closed and you can send it again. A copy or export of your data is a download link that works for 7 days.

9. 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 and asks for your password again 30 days after you last typed it. If you turn on Face ID or fingerprint unlock, your phone checks your face or fingerprint itself: TaxAudit never receives them, and keeps on your phone only whether unlocking is on.
- 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. To help you, our support staff can see your account details: your name and email, your plan, whether your email is confirmed, how many businesses you have (not their names), when you were last active and whether you've allowed support access.
- 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 (taxaudit.ng/security).

10. 10. Complaints

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

11. 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.