

Privacy Policy

Effective date: 2026-07-01 **Last updated:** 2026-09-28

1. Who we are

RetiFlo ("**RetiFlo**", "**we**", "**us**", "**our**") is a retirement planning and analytics service operated by RetiFlo LLC at 4005 Wyndham Dr NE, Cedar Rapids, IA 52402, available at RetiFlo.com(<https://retiflo.com>). This Privacy Policy explains what personal information we collect, how we use and protect it, who we share it with, and the rights you have over it.

This policy covers the RetiFlo web application and marketing site. It does not cover third-party services we link to, which have their own privacy policies.

If you have questions about this policy or your data, contact us at privacy@retiflo.com or through our contact page (<https://retiflo.com/contact>).

2. Information we collect

We collect only what we need to provide the service.

a. Account & identity information

When you register and use your account, we collect: email address, a hashed password (we never store your password in plaintext), and your first name, date of birth, and optionally, your last name, phone number, gender, and U.S. state. If you enable multi-factor authentication (MFA), we store the data needed to verify your second factor.

b. Financial planning information

This is the core of the service. You enter — and we store — the financial details you choose to provide for your retirement plan: assets and investment accounts, income sources, expenses, debts, real estate, healthcare assumptions, Social Security details, pensions, scenarios, and related settings. You control what you enter; you may use the service with as much or as little detail as you wish.

c. Payment information (via Stripe)

If you purchase a paid plan, payments are processed by **Stripe**. We do **not** receive or store your full payment card number — Stripe handles card data directly. We store only Stripe's customer and subscription identifiers and the status of your subscription. See Stripe's privacy policy(<https://stripe.com/privacy>).

d. AI feature data (optional, opt-in)

If you opt in to our AI features, we send **your plan's data with personally identifiable information (PII) removed** to the Anthropic (Claude) API. This can include detailed figures — year-by-year income, expenses, taxes, portfolio values and withdrawal rates, account balances and types, your debts and property values, your ages and retirement dates, when you plan to claim Social Security, and any question you type — because an answer grounded in your own plan requires them.

What never leaves is your identity: names, account and institution names, addresses, email addresses and phone numbers are replaced with neutral placeholders before the request is sent, and restored only in the answer shown back to you. What counts as PII is listed in `pii-classification.md`, which is generated from the code rather than maintained by hand.

AI features are off until you grant consent, and you can withdraw consent at any time in Settings. See §6 for details.

e. Documents you upload

If you choose to use the document vault, we store the files you or your advisor upload — for example a copy of a will, trust or power of attorney. **These files are encrypted before they are stored**, and we hold the key separately from the file. Uploading documents is entirely optional and the service works without it.

A document you upload may contain information about **other people** — an executor, a trustee or a beneficiary named in your will. Please upload only what you are comfortable sharing with us and, where you have chosen to share it, with your advisor.

Our copy is a convenience copy, not the legally operative original. Keep your executed originals where your attorney advises.

f. Bank and card statements you upload for expense analysis

Separate from the document vault above, and handled differently. If you upload a bank or card statement so the service can work out your spending, we parse it into individual transactions and **keep the original file**.

Where it is kept. In our own database, not in the file storage described in (e). **The file is encrypted before the record is written**, with a key held outside the database, so it is unreadable to anyone holding a copy of the database or a backup of it. The filename is encrypted the same way. Our nightly backups are themselves separately encrypted before they leave the server.

Where it is not. The statement is not sent to any third party — not to our payment processor, and not to the AI provider. It is never included in the data sent for the optional AI features described in (d): the third parties and the AI features receive figures, never files.

We keep it for 90 days, and you can remove it sooner. We hold the statement file for 90 days after you upload it so the import can be re-run or a categorization questioned while it is still fresh, and then we delete it; after that window the file has served its purpose. You do not have to wait for it — delete the upload on the **Expenses (Detailed)** screen, or delete your account, and the file is deleted immediately.

Deleting the statement does not delete your spending. The transactions the import produced are your data, not the file's — they stay in your plan and in any budget you built

from them. If you want those gone too, remove them in the expenses screens; they are edited and deleted like anything else you entered by hand.

g. Technical & usage information

To operate and secure the service, we process standard technical data such as your IP address, browser/device information, and authentication session data (we use a signed session cookie to keep you logged in). We send transactional emails (e.g. verification, password reset, notifications) via **Resend** and keep operational delivery logs.

AI usage records. Each time you use an AI feature we record what the request cost us — which feature, which model, how many words were processed, and the date. **Your question and the answer are not part of this record.** It exists so we can apply a daily limit and keep the feature affordable, and we keep it for **12 months**.

Product analytics. We record a small number of events about how the service is used — that an account was created, that a projection finished, that a locked feature was viewed, that a subscription started. **We keep these on our own systems and send them to no one.** They are not used for advertising, we set no cookie for them, and they carry no cross-site identifier. They never contain the figures in your plan, the documents you upload, or anything you type. **They do not involve your browser at all** — our own server records them, so no tracking script runs on your device, and your IP address, browser and device are not part of the record. Each event is labeled with an identifier that exists only for this purpose and is used nowhere else; **deleting your account destroys it**, which leaves the events unlinkable to anyone.

We do **not** sell your personal information, and we do **not** use it for third-party advertising.

3. How we use your information

We use your information to:

- Provide the service — run retirement projections, Monte Carlo simulations, tax and Roth-conversion analysis, and the other analytics you request.
- Create and secure your account, including authentication and MFA.

- Process payments and manage subscriptions (via Stripe).
- Power our AI features — plan insights, the in-app assistant, the Companion ask-line and expense categorization — **only if** you have opted in (via Anthropic).
- Send transactional and service emails (via Resend).
- Maintain, debug, secure, and improve the service.
- Comply with legal obligations and enforce our terms.

4. Legal bases for processing (EEA/UK users)

RetiFlo is offered to residents of the United States only (see the Terms of Service, section 2), so this section will not apply to most people reading it. It is kept because the EU or UK GDPR can still reach someone who is in the EEA or the UK while using the service. Where either applies, we rely on the following legal bases:

- **Performance of a contract** — to provide the service you signed up for.
- **Consent** — for optional features such as AI insights and certain communications; you may withdraw consent at any time.
- **Legitimate interests** — to secure, maintain, and improve the service, where not overridden by your rights.
- **Legal obligation** — to comply with applicable law (e.g. billing/tax records).

5. How we share your information — sub-processors

We share personal information only with the service providers ("sub-processors") necessary to operate RetiFlo, each under a data processing agreement and only for the purposes below. We transmit data to each over encrypted (TLS) connections.

SUB-PROCESSOR	PURPOSE	DATA SHARED
Stripe	Payment & subscription processing	Billing/subscription data; card data handled by Stripe directly

SUB-PROCESSOR	PURPOSE	DATA SHARED
Anthropic (Claude)	AI features (opt-in only): plan insights, the AI assistant, the Companion ask-line, expense categorization	Plan data with PII removed — see pii-classification.md and §6
Resend	Transactional & service email delivery	Your email address and message content
Hetzner	Cloud hosting / infrastructure (United States — Ashburn, Virginia)	Hosts the encrypted application and database

We may also disclose information if required by law, to protect our rights or the safety of others, or in connection with a business transfer (e.g. merger or acquisition), in which case we will notify you as required.

6. AI features and your data

Four features use AI — plan insights, the in-app assistant, the Companion ask-line, and expense categorization. All four are optional, share a single consent, and use the same provider. Every external processor is listed in [data-processors.md](#).

- They are **disabled by default**. Nothing is sent to any AI provider until you explicitly grant consent.
- When enabled, we send **your plan's data with personally identifiable information (PII) removed**. The figures do go: to answer a question about your plan in your own numbers, the model needs those numbers — year-by-year income, expenses, taxes, portfolio values, account balances and types, your debts and property values, your ages and retirement dates, when you plan to claim Social Security, and any question you type.
- **What is removed first**. Before a request leaves our systems, your identifying details — names, account and institution names, addresses, email addresses and phone numbers — are replaced with neutral placeholders such as "that account" or "your spouse". The provider never receives them. Your real wording is restored only in the answer displayed back to you, inside our own systems. Anything not classified as

safe to send is removed rather than sent. The classification is listed in `pii-classification.md` and generated from the code.

- The data is processed by Anthropic under their privacy policy(<https://www.anthropic.com/privacy>).
- You can **withdraw consent at any time** in Settings, which stops further data from being sent.

7. Cookies and sessions

We use a small number of strictly-necessary cookies to keep you signed in and to protect the security of your session. We do **not** use third-party advertising or cross-site tracking cookies. Because these cookies are essential to the service, the site will not function correctly without them.

Our product analytics set no cookie at all. The events described in §2(g) are recorded without one, which is why there is nothing here to consent to or opt out of on that account.

Your financial data is not left behind in your browser after your session ends. We load it into memory only while you are using the app and do not write it to long-term browser storage; when you log out — or after **1 hour of inactivity**, when we automatically log you out — we clear it from your browser. Closing the tab also clears it.

8. Data retention

We keep personal information only as long as needed to provide the service and meet legal obligations:

- **Active account data** is retained while your account is active.
- **When you delete your account**, your account and plan data are **permanently and immediately erased** — there is no soft-delete or recovery period (see §11).
- **Individual records you remove while editing your plan** are hidden from view immediately and retained no longer than **90 days** before permanent deletion.
- **Operational/email delivery logs** are retained for **up to 18 months**.

- **AI usage records** — which feature, which model, how many words and what it cost, but **not your question or the answer** — are retained for **12 months**.
- **Product-analytics events** — which we hold on our own systems and share with no one — are retained for **24 months**.
- **Documents you upload** are kept for as long as your account is active, or until you delete them. Nothing removes them on a schedule. **When you delete a document we destroy the key that makes it readable**, so it cannot be recovered — including from any backup copy that has not yet aged out.
- **Bank and card statements you upload for expense analysis** — the file itself is kept for **90 days**, or deleted immediately if you delete the upload or delete your account. The transactions imported from it are your plan data and stay until you remove them.
- **Encrypted backups** age out in approximately **14 days** and are then permanently deleted; we do not selectively restore individual records.
- **Billing records** held by Stripe are retained per Stripe's obligations (approximately **7 years** for legal/tax purposes).

Our internal retention rules are documented in our Data Retention & Deletion Policy. A copy may be requested by email from privacy@RetiFlo.com.

9. How we protect your information

We apply layered security controls, including:

- **Encryption in transit** — all traffic is served over HTTPS/TLS with HSTS enabled.
- **Field-level encryption** — sensitive fields are encrypted at rest with AES-256.
- **Encryption at rest** — the production database and secrets reside on an encrypted (LUKS) volume.
- **Access controls** — least-privilege database roles, restricted network exposure, and a hardened deployment.
- **Authentication** — hashed passwords and optional multi-factor authentication.

No method of transmission or storage is 100% secure, but we work to protect your information using industry-standard safeguards. Our broader security program is

described in our Information Security Policy. A copy may be requested via email from privacy@RetiFlo.com.

10. Your rights

Depending on where you live, you may have some or all of the following rights:

- **Access** — request a copy of the personal information we hold about you.
- **Correction** — correct inaccurate information (much of which you can edit directly in the app).
- **Deletion / erasure** — request deletion of your personal information (see §11).
- **Portability** — request your data in a portable format.
- **Withdraw consent** — for optional features such as AI insights.
- **Objection / restriction** — object to or restrict certain processing.

California residents (CCPA/CPRA): you have the right to know, delete, correct, and to opt out of "sale" or "sharing" of personal information. We do **not** sell or share your personal information as those terms are defined under California law. We will not discriminate against you for exercising your rights.

To exercise any right, contact us at privacy@retiflo.com. We verify your identity before acting on a request. We respond to verified deletion requests within **30 days** (GDPR/UK GDPR) or **45 days** (CCPA/CPRA), extendable to 90 days where permitted with notice to you.

11. Deleting your account

You can delete your account at any time from your account settings. Here is exactly what happens.

What we delete, and when

Straight away, and permanently. Not marked for deletion, not hidden — removed. That includes your plan and every figure in it, any bank or card statements you uploaded, any

documents in the document vault, your saved scenarios and reports, and your login details.

This cannot be undone, and we cannot recover it for you afterwards. If you want a copy, export your data before you delete.

Our backups. We keep encrypted backups for about 14 days in case of disaster. A backup taken before you deleted your account still contains your data until it ages out. **If we ever have to restore one, your deletion is applied again** so that restoring a backup cannot quietly bring your account back.

What we cancel

If you have a paid subscription, we cancel it with Stripe, our payment processor, as part of the deletion. You are not billed again.

What we cannot delete

Stripe keeps its own record of payments you made. We cannot delete that, and neither can any business that uses Stripe. Payment companies are required by law — tax, accounting and anti-fraud rules — to keep records of transactions for a number of years, and those records belong to Stripe rather than to us.

To be clear about what this does and does not mean:

- **We delete our copy of everything**, including the identifiers that linked you to Stripe. Once your account is gone, we hold nothing that connects you to a payment record.
- **What Stripe holds is a payment history** — that a card paid a subscription — not your retirement plan, your figures or anything you uploaded. None of that is ever sent to Stripe.

If you want to know what Stripe holds, or ask them to act on it, contact Stripe directly.

Their privacy policy explains what they keep and how to reach them:

<https://stripe.com/privacy>.

You are welcome to email us at privacy@retiflo.com if you would like help with that — we will point you to the right place, though the request has to go to Stripe.

12. International data transfers

RetiFlo is hosted in the **United States** (Hetzner, Ashburn, Virginia) and is **offered to US residents only**, so your information is stored and processed in the United States. If you nonetheless access the service from outside the United States, your information will be transferred to and processed in the United States, and by the sub-processors listed in §5, which may be located in other countries. Where required, such transfers are made under appropriate safeguards (e.g. Standard Contractual Clauses).

13. Children's privacy

RetiFlo is intended for adults planning for retirement and is **not directed to children**. We do not knowingly collect personal information from anyone under 18. If you believe a child has provided us information, contact us and we will delete it.

14. Changes to this policy

We may update this policy from time to time. When we make material changes, we will update the "Last updated" date and, where appropriate, notify you. Your continued use of the service after an update constitutes acceptance of the revised policy.

15. Contact us

Questions, requests, or complaints about this policy or your personal information:

- **Email:** privacy@retiflo.com
- **Contact form:** retiflo.com/contact (<https://retiflo.com/contact>)
- **Operator:** RetiFlo LLC, 4005 Wyndham Dr NE, Cedar Rapids, IA, USA 52402

EEA/UK users: if applicable, add EU/UK representative and the right to lodge a complaint with your local supervisory authority.

RetiFlo

Navigate retirement with calm confidence — and a steady hand when you need one.

PRODUCT

[For Individuals](#)

[Personal Plans](#)

[Resources](#)

[Glossary](#)

[Blog](#)

COMPANY

[About](#)

[Contact](#)

[Blog](#)

FOR ADVISORS

[Practice Track](#)

[Marketplace](#)

[Advisor Plans](#)

ACCOUNT

[Log in](#)

[Create account](#)