

Privacy Policy

Effective: August 28, 2026

Owner: Adam Blumberg (CCO) + Nick Rygiel (CTO/CISO)

Contents

Privacy Policy	2
FACTS: What Does Protocol Wealth, LLC Do With Your Personal Information?	2
Why?	2
What?	2
How?	3
Who We Are	4
What We Do	4
Use of AI Tools and Data Privacy	4
Recording and Transcription of Client Meetings	6
Co-Intelligence Framework — How AI and Human Advisers Work Together	6
PW Nexus API and MCP Server	7
Third-Party Financial Data Services	8
Cookies and Tracking Technologies	9
How We Share Information with Third Parties	9
How Does Protocol Wealth Protect My Information?	12
International Clients and Cross-Border Data Processing	13
Data Retention for Advisory Services	13
Your Data Rights	14
Your Rights Regarding AI-Assisted Services	14
Sensitive Personal Information	15
California Privacy Rights (CCPA/CPRA)	15
Why Can't I Limit All Sharing?	16
How Do I Limit Sharing?	16
Definitions	16
Version History	17
Questions?	22

Privacy Policy

Classification: Public. Served at protocolwealthllc.com/privacy. A notice of current practice, not a contract — never pinned; the archive preserves what it said on any date.

Protocol Wealth, LLC

Effective / Last Revised: August 28, 2026 **Owner:** Adam Blumberg, Chief Compliance Officer
Companion: List of Subprocessors (effective August 28, 2026)

This document is identified by its effective date, not a sequential version number. Last updated August 28, 2026; change reference v3.13 — see Version History below for the dated revision log.

This version removes **Octav** from the list of third parties. The firm no longer uses it, and naming a provider we do not use tells you something that is not true. Before removing it we checked rather than assumed: no data ever flowed to Octav — there is no client for it in our systems, no credential wired into them, and no record of a single call to it. Nothing else about what we collect, why, or who else receives it has changed.

FACTS: What Does Protocol Wealth, LLC Do With Your Personal Information?

Why?

Protocol Wealth collects and develops personal information about clients, and some of that information is non-public personal information (Customer Information). The essential purpose for collecting Customer Information is to provide and service the appropriate financial products and services clients obtain from Protocol Wealth.

What?

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and **income**
- **account balances** and **transaction history**
- **assets** and **credit card or other debt**

As an investment adviser, Protocol Wealth collects and develops Customer Information about clients in order to provide investment advisory services. The categories collected depend upon the scope of the engagement and include:

- Information received from clients on financial inventories and questionnaires through consultation with Advisory Representatives, including personal and household information such as income, spending habits, investment objectives, financial goals, statements of account, assets and liabilities, and other records concerning clients' financial condition.

- Information needed to open an account including social security numbers, investment experience, assets, income, and account balances.
- Account data retrieved from the financial institutions a client chooses to link, including account balances, transaction history covering up to the preceding 24 months, investment holdings and investment transactions, and **liabilities — credit cards, student loans, and mortgages**. See “Third-Party Financial Data Services” below for how these connections work and which providers are involved.
- Information developed as part of financial plans, analyses, or investment advisory services.
- Information concerning investment advisory account transactions.
- Information about clients’ financial products and services transactions with Protocol Wealth.

When you are no longer our customer, we continue to share your information as described in this notice.

How?

All financial companies need to share customers’ personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers’ personal information; the reasons Protocol Wealth chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Protocol Wealth share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations	Yes	No
For our compliance with rules and regulations — information about your transactions and communications provided to non-affiliated firms when required	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don’t share

Reasons we can share your personal information	Does Protocol Wealth share?	Can you limit this sharing?
For our affiliates' everyday business purposes — information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes — information about your creditworthiness	No	We don't share
For our affiliates to market to you	No	We don't share
For nonaffiliates to market to you	No	We don't share

Who We Are

Who is providing this notice? Protocol Wealth, LLC — an SEC-registered investment adviser (CRD #335298).

What We Do

Use of AI Tools and Data Privacy

Protocol Wealth uses AI tools as part of a co-intelligence framework that combines human adviser expertise with artificial intelligence under human oversight. AI supports research, analysis, portfolio monitoring, document preparation, and administrative workflows. It does not replace our advisers, make autonomous investment decisions, or operate outside our supervision. Every material AI-assisted output is reviewed by a human adviser before it reaches you or influences a recommendation made on your behalf.

Our primary AI provider is Anthropic, PBC, engaged under a Zero Data Retention agreement. Inputs and outputs sent via the Claude API are not retained by Anthropic beyond request duration; our data is contractually excluded from any use in training or improving AI models; inference is restricted to US-based infrastructure; and outputs are not subject to human review.

A further provider, **xAI Corp. (Grok)**, is engaged today **only for automated source-code review**, which processes our own code and no client data. An advisor-chat capability using Grok is built and provisioned but **not enabled**; no client advisory content reaches xAI today. We name it here before it is enabled as early transparency, and we will update this policy and give notice before that changes. Zero data retention is contracted at the team level and asserted by xAI on every response; our systems verify that assertion on each call and reject any response that does

not carry it, so a change in the retention regime stops the request rather than passing unnoticed. Inference is pinned to a U.S. region by a fail-closed allowlist. xAI publishes that it is SOC 2 Type 2 compliant and states that it never trains on API inputs or outputs without explicit permission; we have not yet obtained its audit report for our vendor file, and our reliance also rests on the contracted retention terms and that per-response check.

Two further AI providers operate in narrower, firm-internal roles, behind the same controls:

- **Google Gemini (Google LLC, Gemini API)** — (a) image and graphics generation for advisor workflows, and (b) automated source-code-review scans as one of the model providers in our internal software-review process. All Gemini calls are brokered through our backend and run on the paid tier of the Gemini API, under which Google does not use our inputs or outputs to train its models and does not subject them to human review; inputs and outputs are subject only to a short abuse-monitoring retention window (approximately 72 hours) and processing is US-based. Client PII is removed before any data reaches Google; the source-code-review path handles only our own source code (not client data) and runs behind a separate pre-egress secret and PII scan.
- **OpenAI** — (a) voice transcription via the Whisper API for advisor-initiated dictation (advisor voice memos transcribed into internal workflows), and (b) automated source-code review via the OpenAI API (Codex) as one of the model providers in our internal software-review process. OpenAI does not use our API data to train its models. Whisper content is limited to what an advisor dictates and is not connected to client accounts or the client portal; the source-code-review path handles only our own source code (not client data) behind a pre-egress secret and PII scan. OpenAI is not used to process client data.

We do not currently operate self-hosted AI models; should external ZDR conditions change, we reserve the ability to deploy self-hosted alternatives and will update this policy before doing so.

The safeguards we apply when AI touches client information:

- Client nonpublic personal information is anonymized, tokenized, or removed before being entered into external AI tools where feasible
- Account numbers, Social Security numbers, and similarly sensitive identifiers are never submitted directly to external AI tools
- AI tool settings are configured to opt out of model training where available, and we prefer providers who contractually commit to no-training terms
- AI-generated content is reviewed by qualified personnel before use in client communications or investment decisions
- AI outputs that affect your account are auditable — we maintain records of AI-assisted work to support compliance review
- We review AI tool terms of use, privacy policies, and data sharing practices before engagement and on an ongoing basis

What AI does not do at Protocol Wealth:

- AI does not make final investment decisions on your behalf without human adviser review

- AI does not override the fiduciary judgment of your investment adviser representative
- AI does not determine your fees, account access, or legal rights under your advisory agreement
- AI-generated outputs that include client data are never sold, syndicated, or shared with third parties for purposes unrelated to serving you

If you use the AI assistant in your client portal, your use is also governed by our AI Acceptable Use Policy, which explains in plain language what the assistant will and will not do, how your data is handled, and how to reach a human on your advisory team.

Recording and Transcription of Client Meetings

We do not record or transcribe client meetings without your consent and advance notice. Advisor-initiated dictation — short voice memos an advisor records for internal note-taking, transcribed into our internal workflows (see the OpenAI / Whisper disclosure above) — does not involve recording your meetings with us. Where we hold the technical ability to record or transcribe a video meeting (for example, through our Google Workspace conferencing tools), we will notify you before any meeting is recorded or transcribed and will proceed only with the consent of the participants, consistent with applicable two-party-consent expectations. You may decline recording at any time.

Co-Intelligence Framework — How AI and Human Advisers Work Together

The core of our approach is that AI and human advisers guard each other rather than replace each other:

- **AI as a guardrail on advisers.** AI provides 24/7 monitoring, flags portfolio drift, identifies concentration risk, performs consistency checks on advisory outputs, and produces double-checks on numerical work. If an adviser misses something, AI is positioned to catch it.
- **Human advisers as a guardrail on AI.** Every material AI-assisted output is reviewed by a registered investment adviser representative before it reaches you or influences an action on your behalf. AI can produce plausible-looking but incorrect outputs (“hallucinations”). Human review catches these before they become problems.
- **AI excels at persistent, repetitive work.** Continuous monitoring of portfolios, regime detection, document summarization, research synthesis, compliance screening. These tasks benefit from AI’s tireless consistency.
- **Human advisers excel at judgment, relationship, and fiduciary obligations.** Understanding your life circumstances, weighing tradeoffs that don’t reduce to numbers, exercising the duty of care that is legally and ethically ours to bear. These are not delegated to AI.

This dual-guardrail approach is how we preserve the fiduciary relationship while making use of technology that genuinely improves our service quality.

PW Nexus API and MCP Server

Protocol Wealth operates PW Nexus (nexusmcp.site), a research API and Model Context Protocol (MCP) server that provides investment analysis tools, market data, and portfolio analytics. This section describes data practices specific to API and MCP server usage.

Data collected from API and MCP users:

- **Authentication data:** Email address, OAuth tokens, and session identifiers used to authenticate your access. OAuth tokens issued by our authorization server (pwportal.app for clients, pwos.app for advisor personnel) are encrypted in transit and stored with standard security controls.
- **Usage logs:** Tool invocations, API endpoint requests, timestamps, IP addresses, and request metadata. These logs are used for rate limiting, abuse prevention, service reliability, and debugging.
- **Query data:** Ticker symbols, wallet addresses, and other parameters you submit when using API endpoints or MCP tools. Query data is processed to return results and may be cached temporarily to improve performance.

How API and MCP data is used:

- To provide and improve the API and MCP services
- To enforce rate limits and prevent abuse
- To diagnose technical issues and maintain service reliability
- To generate aggregate, non-identifying usage statistics

How API and MCP data is NOT used:

- API and MCP usage data is never sold to third parties
- Query parameters and tool invocations are not used to build individual user profiles for marketing purposes
- Non-client API usage data is not shared with third parties except as required by law

Data retention for API and MCP usage:

- **Non-advisory access logs** (IP addresses, request timestamps, rate-limiting metadata for non-client, non-advisory interactions): retained for 90 days, then automatically purged.
- **Advisory-related interactions** (tool invocations by Clients that constitute or relate to investment advisory communications): retained for a minimum of five (5) years in accordance with SEC Rule 204-2.
- **Authentication tokens:** retained for the duration of the session or until revoked.
- **Cached query results:** retained according to cache TTL policies (ranging from 30 seconds to 24 hours depending on data type).

Accessing PW Nexus through third-party AI platforms:

When you connect to PW Nexus via an MCP connector in a third-party AI assistant (such as Claude, Cursor, or similar MCP-compatible platforms), your queries and our responses are transmitted through that platform's infrastructure. Protocol Wealth applies automated PII filtering to

API and MCP responses to prevent client nonpublic personal information from being transmitted through third-party platforms.

However, Protocol Wealth does not control how third-party platforms process, cache, or retain data transmitted through their systems. Users accessing PW Nexus through third-party platforms should review that platform's privacy policy.

Advisory clients should not submit nonpublic personal information (such as account numbers, Social Security numbers, or detailed financial data) through third-party AI platforms or MCP connectors. For communications involving sensitive account information, please use the client portal (pwportal.app) or contact your advisor directly.

Third-Party Financial Data Services

To provide account aggregation, cashflow analysis, and portfolio reporting to advisory clients, Protocol Wealth uses third-party financial data services to securely connect to your external financial accounts. These services are available exclusively to clients who have executed an Investment Advisory Agreement with Protocol Wealth ("Clients") and are used solely to provide advisory services. Account data retrieved through these services is not shared with, sold to, or made accessible to any third party for their independent use.

Prospective clients ("Prospects") and general users of Protocol Wealth digital properties do not have access to account linking or financial data aggregation features. Access to aggregation services requires both authentication and verified Client status.

Currently active third-party data service providers:

- **Quiltt, Inc.** — provides a unified data aggregation platform that connects to financial institutions on our behalf. Quiltt is used exclusively for Client account aggregation within the advisory relationship. Quiltt's privacy policy: <https://www.quiltt.io/policies/privacy-policy>
- **MX Technologies, Inc.** — provides financial institution connectivity through Quiltt's aggregation platform. MX's privacy policy: <https://www.mx.com/privacy-policy>
- **Finicity, Inc. (a Mastercard company)** — provides financial institution connectivity through Quiltt's aggregation platform. Finicity's privacy policy: <https://www.finicity.com/privacy/>
- **FinGoal** — provides transaction data cleaning and enrichment through Quiltt's aggregation platform. FinGoal's privacy policy: <https://fingoal.com/privacy>

Connectivity with **Plaid, Inc.** is in progress via our Quiltt integration. Plaid is named here in advance of enablement so that this notice, and the companion List of Subprocessors, precede rather than follow the change. No client data flows through Plaid today.

What the connection collects. When you link an account, the secure interface collects your **email address** and no other profile field — not your name, phone number, mailing address, or date of birth. The account data retrieved is:

- **Account balances and transaction history**, covering up to the preceding **24 months**. This is required for every linked account.
- **Investments** — holdings and investment transactions.
- **Liabilities** — credit cards, student loans, and mortgages.

You initiate all account connections through a secure interface provided by these services within the client portal (pwportal.app). Protocol Wealth does not receive or store your banking login credentials. You may disconnect any linked account at any time through the client portal or by contacting your advisor.

Financial data retrieved through these services is:

- Encrypted in transit (TLS 1.2+) and at rest (AES-256)
- Stored only for the purpose of providing Advisory Services
- Never sold to third parties
- Never shared with or accessible to non-Client users of Protocol Wealth digital properties
- Subject to our data retention schedule (retained per SEC requirements, securely disposed when no longer required)

Cookies and Tracking Technologies

Protocol Wealth uses cookies and similar technologies only as necessary to operate our digital properties securely. We do not use third-party advertising, marketing, or cross-site tracking cookies, and we do not sell or share personal information for cross-context behavioral advertising.

- **Strictly necessary cookies.** Our authenticated client and advisor portals (pwportal.app, pwos.app) set first-party session and authentication cookies that are required to sign you in, keep your session active, and protect that session. These cannot be disabled without breaking core functionality.
- **Security and infrastructure cookies.** Our public website is served through Cloudflare, which sets short-lived, strictly necessary cookies (for example, `__cf_bm` for bot management and `__cflb` for load balancing) to keep the site secure and available.
- **No advertising or cross-site tracking.** We do not embed third-party advertising pixels, retargeting tags, or cross-site trackers on any Protocol Wealth property.

Because we use only strictly necessary cookies, no consent banner is required. You may control or block cookies through your browser settings, although disabling strictly necessary cookies will prevent you from signing in to the portals. If we introduce analytics or any non-essential tracking technologies in the future, we will update this section and provide any choices or opt-outs required by applicable law, including recognition of Global Privacy Control (GPC) signals where required.

How We Share Information with Third Parties

To administer, manage, and service client accounts, process transactions, and provide related services, Protocol Wealth provides access to Customer Information to non-affiliated companies, other

investment advisers, custodians, and financial institutions. Third-party service providers who may receive Customer Information include:

Custody, Brokerage, Trading, and Billing

- Altruist Financial LLC — advisory billing and custody
- Charles Schwab & Co., Inc. — qualified custodian for advisory accounts held on Schwab Advisor Services; holds client assets, executes trades, and produces the official books and records and client statements for those accounts
- Performance Technologies, Inc. d/b/a Schwab Intelligent Technologies — operates Schwab OpenView Gateway. Account and position data we request for delivery into a system we use is replicated and maintained in a database at this entity before it is delivered. It is a separate company from Charles Schwab & Co., Inc., though both are subsidiaries of The Charles Schwab Corporation
- Interactive Brokers LLC — brokerage
- Anchorage Digital Bank — qualified digital asset custodian (federally chartered)
- FalconX — digital asset trading / execution provider in a tri-party arrangement where Anchorage Digital Bank remains the qualified custodian
- BitGo Trust Company — qualified digital asset custodian
- Fordefi — multi-party computation (MPC) wallet infrastructure for onchain holdings
- Coincover — independent third-party backup key holder for MPC wallet recovery

Financial Planning

- RightCapital, Inc. — financial planning platform. Your advisory agreement provides access to RightCapital or a similar online platform for financial modeling and portfolio analysis, and your written plan may be delivered through it. The information a plan is built from — household details, income, expenses, account balances and holdings, goals, insurance, and tax assumptions — is held there
- Monarch Money — cash-flow management and expense tracking, named in your advisory agreement as part of the planning service. **We do not send Monarch any information about you.** You hold your own Monarch account and connect your own financial institutions to it. Where you choose to share a transaction export from it, your adviser imports that file into our systems. It is named here so that a provider your advisory agreement mentions is one you can find in this notice

Financial Data Aggregation

- Quiltt, Inc. — financial account aggregation platform (orchestrator)
- MX Technologies, Inc. — connectivity through Quiltt (currently active)
- FinGoal — data cleaning and enrichment through Quiltt (currently active)
- Finicity, Inc. (a Mastercard company) — connectivity through Quiltt (currently active)

AI Services

- Anthropic, PBC — primary AI provider; Claude API under a Zero Data Retention agreement (US-only inference, no model training on our data, no human review)

- Google LLC — Gemini API for (a) advisor-facing image and graphics generation and (b) automated source-code-review scans (paid tier: no model training on our data, no human review; ~72-hour abuse-monitoring retention; US-based; brokered through our backend behind our PII redaction pipeline and egress controls)
- xAI Corp. — Grok API as an independent second source-code reviewer (our own source code; **no client data**). An advisor-chat capability is built and provisioned but not enabled, and no client advisory content reaches xAI today. Team-level zero data retention is asserted per response and verified by our systems; U.S. region-pinned; SOC 2 Type 2 published by the vendor, audit report not yet obtained for our file
- OpenAI — Whisper API for advisor-initiated voice-memo transcription and the OpenAI API (Codex) for automated source-code review (no model training on our data; source-code review processes our own code, not client data, behind a pre-egress secret and PII scan; not connected to client accounts)

Infrastructure and Platform

- Google Cloud Platform and Google Workspace — compute, email, document storage, productivity, and identity services under Google’s business and enterprise terms
- Cloudflare — DNS, content delivery, web application firewall, and network security

Identity Verification and Compliance

- Veriff — identity verification during onboarding (used for clients whose identity is not verified through a custodian’s onboarding flow, including DeFi/crypto-only clients)
- Scorechain S.A.S. (via QuickNode) — blockchain sanctions screening (Scorechain Free Sanctions API: OFAC and international sanctions lists applied to onchain wallet addresses) and Know Your Transaction / Know Your Wallet risk scoring (Scorechain Risk Assessment API via QuickNode). Only public onchain identifiers are transmitted; no client PII.
- QuickNode, Inc. — multi-chain RPC and blockchain-data infrastructure; the substrate carrying the Scorechain Risk Assessment API and general onchain reads (public onchain identifiers only)
- Hadrius — compliance monitoring and supervision (trade surveillance, marketing review, communication archiving)

Communications and Documents

- Wealthbox — customer relationship management (CRM)
- Postmark — transactional email delivery
- Anvil — document signing services

Onchain Data

- DeBank — multi-chain wallet and DeFi position data (primary onchain position-data source; read-only, public onchain data only)
- Helius Blockchain Technologies, Inc. — Solana RPC and indexed-history reconstruction (read-only public wallet/account/transaction identifiers and request metadata only; no signing or transaction submission)

- Blockstream Corporation (Blockstream.info / Esplora) — Bitcoin address-balance lookup (read-only public wallet address and request metadata only; no signing or transaction submission)

A current list of service providers is maintained at protocolwealthllc.com/subprocessors and available on request. All third-party providers are subject to our vendor risk assessment process and contractual data protection requirements.

Protocol Wealth may also provide Customer Information outside the firm as permitted by law — for example, to government entities or other third parties in response to subpoenas, regulatory examinations, or similar legal processes. **We do not share Customer Information with affiliates or non-affiliated third parties for marketing purposes. We do not sell client information. We do not authorize our service providers to use client information for purposes other than providing services to us.**

How Does Protocol Wealth Protect My Information?

To protect your personal information from unauthorized access and use, we maintain an information security program that complies with federal law, including:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Multi-factor authentication for system access
- Role-based access controls limiting data access to authorized personnel
- Immutable audit trail logging all access to client data
- Incident response program for detecting and responding to security events
- Regular security assessments of third-party service providers
- Due diligence and monitoring of third-party service providers who have access to client information
- Automated PII filtering on API and MCP responses to prevent inadvertent disclosure of client information through programmatic interfaces
- **Tenant isolation at the database level** — client data is isolated from other clients' data through database-engine-level row-level security policies. This is a structural control that prevents cross-client data exposure even in the event of application-layer errors.
- **AI data handling controls** — external AI services are engaged under terms that prohibit use of our data for model training. Our primary AI provider (Anthropic) additionally operates under a Zero Data Retention agreement with US-only inference. See the “Use of AI Tools and Data Privacy” section above for the specifics of each AI service we use.
- **Data residency in the United States** — client data storage occurs on infrastructure located within the United States. Our primary storage and processing is within Google Cloud Platform (US regions). External AI inference with our primary AI provider (Anthropic) is contractually restricted to US regions.
- **Segregation of sensitive data from external AI** — client nonpublic personal information is segregated from external AI workflows through our PII filtering pipeline. Where AI

assistance is applied to client-identified data, the data passes through redaction controls that replace identifiers with placeholder tokens before external transmission.

In the event of a data security incident involving unauthorized access to your sensitive customer information, we will notify you as soon as practicable, but no later than 30 days after becoming aware of the incident, in accordance with SEC Regulation S-P as amended.

International Clients and Cross-Border Data Processing

Protocol Wealth serves a limited number of non-U.S. clients, including entity and individual clients in jurisdictions such as Singapore and the United Arab Emirates. If you are located outside the United States, you should understand that:

- Your personal information is processed and stored on infrastructure located in the **United States** (primarily Google Cloud Platform, US regions), and external AI inference with our primary AI provider is contractually restricted to US regions. We do not maintain client-data processing in your country of residence.
- Because your information is stored and processed in the United States, it is subject to **U.S. law**, including lawful access by U.S. government authorities under U.S. legal process, and the United States may not provide the same level of data-protection or privacy rights as your country of residence. By entering into an advisory relationship and using our Services, you consent to this transfer and processing.
- Non-U.S. relationships are additionally subject to our **OFAC / sanctions screening, FATCA, and (where applicable) CRS** procedures, and to the international / non-U.S. terms of your Investment Advisory Agreement, which control the cross-border aspects of the relationship.
- Crypto-only non-U.S. engagements are scoped to the digital-asset advisory services described in your Investment Advisory Agreement; we do not provide services we are not registered or permitted to provide in your jurisdiction.

If you have questions about cross-border processing, contact privacy@protocolwealthllc.com.

Data Retention for Advisory Services

We retain client information for the duration of the advisory relationship plus the period required by applicable law and regulation:

- **Advisory records required under Investment Advisers Act of 1940 Rule 204-2** — at least 5 years from the end of the fiscal year in which the record was created, with the first 2 years in an easily accessible location
- **Audit logs (sanitized of identifying information)** — at least 7 years
- **Identity verification and sanctions screening records** — per applicable vendor defaults and compliance requirements, typically 7 years
- **Transactional email and document signing records** — 7 years

- **AI-assisted research outputs that become part of an advisory record** — subject to Rule 204-2 retention; retained consistent with the related advisory record

When the required retention period expires, we delete or anonymize the data. Certain derivative data (anonymized analytics, system telemetry without client identifiers) may be retained longer for operational purposes.

Your Data Rights

You have the right to:

- **Access:** Request a copy of the personal information we hold about you
- **Correction:** Request correction of inaccurate information
- **Deletion:** Request deletion of your personal information, subject to regulatory retention requirements (certain records must be retained for 5 years per SEC Rule 204-2)
- **Disconnect accounts:** Remove any linked financial account connection at any time through the client portal or by contacting your advisor
- **Revoke API access:** Revoke any API keys or OAuth tokens associated with your account at any time through the client portal or by contacting your advisor
- **Opt out:** Opt out of certain information sharing as described below

To exercise any of these rights, contact us at privacy@protocolwealthllc.com or security@protocolwealthllc.com. We will respond to verified requests within 30 days. Some requests may be subject to regulatory exceptions — for example, we cannot delete records that SEC regulations require us to retain.

Your Rights Regarding AI-Assisted Services

You have rights regarding how AI is used in connection with your account:

- **Explanation of human review.** If an AI-assisted output affects your account or advisory experience, you may ask your adviser to walk through the human review that occurred before the output was acted on. We will provide that explanation promptly.
- **Inquiry into AI involvement.** You may ask what AI tools were involved in any specific analysis, report, or recommendation you received from us. We will tell you.
- **Opt-out from external AI processing.** If you prefer that your data not pass through external AI services, contact your adviser to discuss. This applies to **every** external AI service we use — including any provider added after you ask — not only the ones named in this policy on the day you read it; the current list is always in our List of Subprocessors. We will describe which services remain available without external AI, any operational implications (for example, certain analyses may take longer or be structured differently), and any cost implications. We will not penalize you for choosing this option.
- **Opt-out from all AI-assisted workflows.** You may request that no AI tools be used in work related to your account. This request will be accommodated to the extent feasible, and we will discuss the scope and implications with you.

These rights are in addition to the data rights described in “Your Data Rights” above.

Sensitive Personal Information

Some of the information we collect is **Sensitive Personal Information** — the categories that receive heightened protection under privacy laws such as the California Privacy Rights Act (CPRA). For Protocol Wealth, Sensitive Personal Information includes:

- Social Security numbers, taxpayer identification numbers, and other government-issued identifiers;
- financial account numbers and the access credentials or tokens used to reach a financial account;
- precise financial and transactional data, including account balances, holdings, transaction history, and outstanding debt (credit card, student loan, and mortgage balances and payment history).

We use Sensitive Personal Information only as necessary to provide the Services, to meet our legal and regulatory obligations, and for other purposes permitted by law. We do not use it to infer characteristics about you, and we do not sell it or “share” it for cross-context behavioral advertising. As described in “Use of AI Tools and Data Privacy” above, account numbers, Social Security numbers, and similarly sensitive identifiers are never submitted directly to external AI tools, and client identifiers are removed or tokenized before any AI processing.

California Privacy Rights (CCPA/CPRA)

Most of the personal information Protocol Wealth holds about advisory clients is financial information collected in the course of providing financial services. That information is regulated under the Gramm-Leach-Bliley Act (GLBA) and is exempt from the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA); it is governed by the “FACTS” notice and the other sections of this Privacy Policy.

The CCPA/CPRA does, however, apply to personal information we collect from California residents who are **prospects or website visitors** — for example, information submitted through our contact forms, diagnostics, and risk questionnaires — that is not collected under the GLBA. If you are a California resident, you have the right to:

- **Know and access** the categories and specific pieces of personal information we have collected about you, the sources of that information, the business purpose for collecting it, and the categories of third parties with whom we share it;
- **Delete** personal information we have collected from you, subject to legal and regulatory retention exceptions;
- **Correct** inaccurate personal information we maintain about you;
- **Opt out of the sale or “sharing”** of personal information for cross-context behavioral advertising; and
- **Not receive discriminatory treatment** for exercising any of these rights.

We do not sell your personal information, and we do not “share” it for cross-context behavioral advertising, so there is nothing to opt out of today; if that ever changes, we will update this policy and provide the opt-out mechanisms the law requires. Where we are required to honor them, we recognize **Global Privacy Control (GPC)** browser signals as a valid opt-out request. You may exercise these rights yourself or through an **authorized agent**, and you may submit a request by contacting privacy@protocolwealthllc.com. We will take reasonable steps to verify your request, respond within the timeframes required by law, and will not require you to create an account in order to make a request.

Why Can't I Limit All Sharing?

Federal law gives you the right to limit only:

- Sharing for affiliates' everyday business purposes — information about your creditworthiness
- Affiliates from using your information to market to you
- Sharing for nonaffiliates to market to you

State laws and individual companies may give you additional rights to limit sharing.

How Do I Limit Sharing?

If you choose to opt out now, at any time in the future, or wish to withdraw your opt out request, contact us at privacy@protocolwealthllc.com. If it is your choice to opt out, there will be a 30-day period before your opt out will take effect.

Definitions

Affiliates: Companies related by common ownership or control. They can be financial and nonfinancial companies. Protocol Wealth does not share with affiliates.

Nonaffiliates: Companies not related by common ownership or control. They can be financial and nonfinancial companies. Protocol Wealth does not share with nonaffiliates so they can market to you.

Joint Marketing: A formal agreement between nonaffiliated financial companies that together market financial products or services to you. Protocol Wealth may enter into joint marketing agreements with other financial companies. **Protocol Wealth does not share your personal information with those companies for joint marketing purposes**, which is why the table above answers “No” for joint marketing.

Client: An individual or entity that has executed a written Investment Advisory Agreement with Protocol Wealth, LLC.

Prospect: A registered user of a Protocol Wealth digital property who has not executed an Investment Advisory Agreement.

Version History

- **v3.13** (effective August 28, 2026) — **Octav removed.** It was listed as a backup source of public on-chain position data, standing behind DeBank. The firm no longer uses it. Naming a provider that does not receive your information is a statement that goes stale the moment anything changes, so it comes off rather than being left as harmless surplus. **The engagement was verified before removal, not assumed:** there is no Octav client and no credential binding in the systems that would call it, and the firm’s audit record holds **zero** Octav events against 33,704 on-chain events overall — so no client information, public or otherwise, ever reached it. Two unused credentials remain in the firm’s secret store pending an operator deletion, and the database migrations that mention Octav are dated records and are not edited. No category of information collected or shared changes, and the geography of processing is unchanged. Companion to List of Subprocessors effective August 28, 2026 (v1.16).
- **v3.12** (effective August 27, 2026) — **Four providers named that were already part of the service and were missing from this notice. No change to what we collect or why.** (1) **Charles Schwab & Co., Inc.** — the qualified custodian for advisory accounts on Schwab Advisor Services. Every other custodian the firm uses was named here; Schwab was not, which was an omission rather than a decision. (2) **Performance Technologies, Inc. d/b/a Schwab Intelligent Technologies** — the firm enrolled in Schwab OpenView Gateway on August 27, 2026 so that Schwab account balances and position detail appear in the customer relationship management system advisers use. Under that enrollment agreement the requested data is replicated and maintained in a database at this entity before delivery, so it is named separately from the custodian: it is a distinct company holding its own copy, and naming only the custodian would understate where client data rests. (3) **RightCapital, Inc.** — the financial planning platform. The firm holds a full diligence package for it, and the Client Advisory Agreement commits to delivering the written plan through it and providing client access to it, so client planning data has always flowed there; it was named in the agreement but not in this notice. (4) **Monarch Money** — named because the same advisory agreement names it. **Protocol Wealth transmits nothing to Monarch,** and the entry says so first: a client holds their own account, connects their own institutions, and the only flow is inbound to us when a client or adviser uploads an export. On a strict reading Monarch is not a service provider receiving client information at all, and it is listed anyway so that a provider named in a client’s own agreement can be found in this notice — the same choice already recorded for Coincover. **Monarch’s published security material attributes a SOC 2 Type 2 report to the data-aggregation provider behind its bank connections rather than to Monarch itself, and this firm does not restate it as Monarch’s own.** A new **Financial Planning** heading is added for the two planning providers. This version reconciles the named roster to the companion List of Subprocessors

effective August 27, 2026; no new category of information is collected or shared, and the geography of processing is unchanged.

- **v3.11** (effective August 25, 2026) — **xAI Corp. (Grok) named on the AI Services roster ahead of engagement; engaged today for source-code review only, with the advisor-chat capability built and provisioned but not enabled.** Previously this policy described one primary AI provider (Anthropic) plus “two additional AI providers ... in narrower, firm-internal roles.” xAI Corp. (Grok) is engaged as an independent second source-code reviewer, processing the firm’s own code and no client data, and an advisor-chat capability using Grok is built and provisioned but **not enabled**. The AI narrative and the third-party sharing list now name xAI in advance of that second engagement, state plainly that no client advisory content reaches it today, and preserve the notice obligation owed before the surface is enabled. **A same-day earlier revision of this entry wrongly described xAI as already receiving client advisory content; it does not, and the error is corrected here rather than silently amended.** Zero data retention for xAI is contracted at the team level and asserted per response; our systems verify that assertion on every call and reject any response lacking it. Inference is U.S. region-pinned by a fail-closed allowlist. xAI publishes SOC 2 Type 2 compliance and states it does not train on API inputs or outputs without explicit permission; the firm has not yet obtained that audit report for its vendor file, and this policy says so. (An earlier same-day draft of this entry wrongly stated that no attestation existed for the vendor; corrected before publication.) **The opt-out right was also corrected:** it previously read “external AI services (such as Anthropic’s Claude API)”, which made a client right depend on a reader deciding which half of the sentence was operative. It now states expressly that the opt-out applies to every external AI service, including any provider added after a client asks — a client who exercised that right against Anthropic is covered against providers that were not on the roster when they asked. No change to what data is collected or to the categories shared. Companion to List of Subprocessors effective August 25, 2026.
- **v3.10** (effective August 14, 2026) — **Republished so the published artifacts match their source. No change to any operative disclosure.** Two artifacts derived from the v3.9 release — the retained PDF and the published page at protocolwealthllc.com/privacy — were produced from a pre-final draft and did not match the v3.9 canonical text they were published with. On the Plaid paragraph, the canonical text said the advance notice **does not discharge** the Subprocessors Inventory’s 30-day advance-notice obligation, which remains owed and is delivered by email to each client account before Plaid is enabled; both derived artifacts instead said the notice discharged that obligation. The canonical text was correct throughout and is unchanged. Because a published version is immutable once archived, the v3.9 record and its retained PDF are left exactly as published and this version supersedes them, rather than either artifact being corrected in place. **Clients who read the v3.9 PDF or the published page between August 13 and August 14, 2026 should read this version: the 30-day advance-notice obligation was not, and is not, discharged by naming Plaid in advance.** It remains owed and is delivered by email to each client

account before Plaid is enabled. The operative text is otherwise unchanged from v3.9, and the vendor roster is unchanged. Companion to Subprocessors Inventory v1.12.

- **v3.9** (effective August 13, 2026) — **Account-aggregation data-flow precision, connectivity-roster reconciliation, and two GLBA sharing-row corrections.** (1) **Liabilities disclosed as a collected data category.** The firm’s aggregation connector retrieves credit-card, student-loan, and mortgage account data, and no prior version of this notice named a debt category. The “What?” summary now carries the Regulation S-P model-form term “**credit card or other debt**”; the Third-Party Financial Data Services section names liabilities explicitly; and the Sensitive Personal Information enumeration adds outstanding debt. This closes a disclosure gap between the live connector configuration and the notice — no change to what is collected, only to what is disclosed. (2) **Collection scope stated precisely** — transaction history covers up to the preceding **24 months**, and account linking collects the client’s **email address** and no other profile field. (3) **Connectivity and enrichment roster reconciled to the live configuration.** **MX Technologies, Inc.** and **Finicity, Inc. (a Mastercard company)** provide institution connectivity; **FinGoal** provides transaction enrichment. MX’s enrichment capability is deliberately not enabled, so MX is described as a connectivity provider only. Finicity moved from the “available on plan upgrade / not currently active” note into the active roster following the firm’s upgrade to the Quiltt Startup plan, whose unlimited-aggregator and fallback-routing terms provision Finicity under the existing Quiltt Master Services Agreement without a separate contract. Akoya LLC remains unengaged and is not listed. (4) **Removed the negative assurance “Protocol Wealth does not currently use Plaid”** in favor of an affirmative statement: connectivity with **Plaid, Inc.** is in progress via the Quiltt integration. Plaid is named in advance of enablement so that this notice and the companion List of Subprocessors precede the roster change rather than follow it. This is early transparency and **does not discharge** the Subprocessors Inventory’s 30-day advance-notice obligation, which is delivered by email to each client account and remains owed before Plaid is enabled. (5) **Two sharing-table rows corrected** — “For joint marketing with other financial companies” and “For our affiliates’ everyday business purposes — information about your transactions and experiences” each changed from “Yes | No” to “**No | We don’t share.**” Protocol Wealth shares no client information with affiliates or with joint marketing partners, so the prior “Yes” values overstated the firm’s sharing. Note the joint-marketing row asks whether the firm **SHARES** for that purpose, not whether it jointly markets — the firm does enter joint marketing agreements and shares nothing under them. All eight rows carry permitted model-form values. The joint-marketing row answers the question the model form actually asks — whether the firm **shares personal information** for joint marketing under the Regulation S-P §248.13 joint-marketing exception — not whether the firm engages in joint marketing at all. Protocol Wealth **does** enter into joint marketing agreements and shares **no** client information under them, so “No | We don’t share” is correct. The **Definitions** section now states both halves explicitly and points at the table, because stating only the first half left the two sections reading as a contradiction. **Note for the CCO:** the model form supplies exactly two sentences for this box — partners are listed, or the firm “doesn’t jointly market” — and neither

fits a firm that jointly markets while sharing nothing. The wording here is accurate rather than prescribed, and that trade-off is flagged for ratification. Companion to Subprocessors Inventory v1.12.

- **v3.8** (effective July 18, 2026) — **Onchain provider-roster reconciliation to List of Subprocessors v1.11.** Added Helius Blockchain Technologies, Inc. for read-only Solana RPC/indexed history and Blockstream Corporation for read-only Bitcoin address-balance lookup. Both receive public onchain identifiers and request metadata only; no direct Client PII, credentials, signing keys, transaction-submission authority, or custody authority is added. Jupiter, Sanctum, and DeFiLlama remain wallet-independent market/reference-data sources rather than client-data subprocessors; Figment and Marinade are identified from public chain state and are not called as PW data processors. No new data category, geography class, or AI service is introduced. The Privacy Policy’s substantive data-sharing scope is unchanged; the named roster now matches Subprocessors v1.11.
- **v3.7** (effective July 2, 2026) — **Client-facing legal refresh: international, California, sensitive-data, and recording disclosures.** Added four sections and one cross-link, closing gaps identified in the 2026-07-02 legal-docs gap analysis versus mature RIA comparables. (1) A new **International Clients and Cross-Border Data Processing** section for our non-U.S. clients (US data residency and processing; consent to US processing and U.S. legal jurisdiction; OFAC / sanctions / FATCA / CRS screening; the Investment Advisory Agreement controls the cross-border relationship). (2) A new **California Privacy Rights (CC-PA/CPRA)** section granting the CPRA rights (know/access, delete, correct, opt out of sale and “sharing,” non-discrimination; GPC honored; authorized-agent requests) for California prospect and website-visitor data, while noting the GLBA exemption for advisory-client financial data. (3) A new **Sensitive Personal Information** enumeration (SSNs/TINs, financial account numbers and credentials, precise financial/transactional data) with a CPRA-style use-limitation. (4) A new **Recording and Transcription of Client Meetings** statement (we do not record or transcribe client meetings without consent and advance notice; two-party-consent posture). (5) A cross-link to the client-portal **AI Acceptable Use Policy** in the AI section. No new categories of client data are shared and there is no vendor-roster change; the AI-provider and subprocessor disclosures remain reconciled to List of Subprocessors v1.8. Companion to Subprocessors Inventory v1.8.
- **v3.6** (effective July 2, 2026) — **Vendor-roster and AI-disclosure reconciliation to List of Subprocessors v1.8.** (1) Reconciled the account-aggregation roster to the providers actually active today — **Quiltt + MX + FinGoal** — and moved **Finicity** and **Akoya** to a “not currently active / available on plan upgrade” note (both had been listed as active connectivity providers but no client data flows through them today), matching Subprocessors v1.8. (2) Corrected and expanded the AI-provider disclosures: the **OpenAI** entry now discloses **both** its Whisper voice-memo transcription use **and** its OpenAI-API (Codex) automated source-code-review use; the **Google Gemini** entry now discloses **both** graphics generation **and** source-code-review scans, with the paid-tier no-training / no-human-review terms, the ~72-hour abuse-monitoring retention window, and US-based processing. Both AI code-review paths process only the firm’s own source code (no client data) behind a pre-egress secret and

PII scan. Anthropic remains the primary provider (ZDR, US-only inference, no training, no human review). (3) **No Plaid** — Plaid Link is not enabled and Plaid is not added as a vendor; Anvil (document signing) and Postmark (transactional email) remain disclosed under “Communications and Documents.” No new categories of client data are shared as a result of this version. Companion to Subprocessors Inventory v1.8.

- **v3.5** (effective June 11, 2026) — Added **FalconX** to the named third-party sharing roster as a digital asset trading / execution provider in a tri-party arrangement where **Anchorage Digital Bank remains the qualified custodian**. No change to the AI disclosures, cookies posture, or account-aggregation scope. Companion to the Subprocessors list.
- **v3.4** (effective June 11, 2026) — AI-disclosure update closing the Gemini live-vs-disclosed mismatch flagged in v3.3 (“Google Gemini not added until its capability ships” — the brokered Gemini capability went live June 4-5, 2026). Added **Google LLC (Gemini API)** (advisor-facing image and graphics generation, brokered through our backend behind the firm’s PII redaction pipeline and egress controls; paid-tier no-training/no-human-review terms; added under the firm’s documented AI-use and vendor-governance review process) and **OpenAI (Whisper)** (advisor-initiated voice-memo transcription only; no chat or reasoning models) to the AI disclosures and the third-party sharing list. Scoped the AI data-handling and data-residency statements so the Zero Data Retention and US-only-inference claims attach to Anthropic specifically. Companion to the Subprocessors list.
- **v3.3** (June 2026; consolidated into v3.4) — Vendor reconciliation to the current Subprocessors inventory + new disclosures. Removed **Chainalysis** (onchain sanctions screening decommissioned 2026-05-29) and replaced it with **Scorechain S.A.S. (via QuickNode)** for sanctions + KYT/KYW screening, plus **QuickNode, Inc.** as the RPC/addon substrate. Removed **Zapper** (never integrated) and added **Octav** as the onchain position-data backup; annotated **DeBank** as the primary onchain source. Added **Finicity (a Mastercard company)** and **Akoya LLC** as Quiltt-routed account-connectivity providers (USAA + coverage gaps). Added a new **Cookies and Tracking Technologies** section (strictly-necessary cookies only; no advertising/cross-site trackers; no banner required). No change to AI disclosures (Anthropic-only; Google Gemini not added until its capability ships).
- **v3.2** (May 3, 2026) — Added co-intelligence framework, Anthropic ZDR disclosure with US-only inference and no-training commitments, corrected vendor list (Quiltt + MX + FinGoal; no Plaid), added Anthropic / Google Cloud / Cloudflare / Hadrius / Anchorage / BitGo / Coincover / Altruist / IBKR / Veriff / Chainalysis / DeBank / Zapper, tenant isolation disclosure, AI data handling controls, US data residency, PII segregation, advisory-level retention schedule, AI-specific client rights. Updated portal references from pwdashboard.com to pwportal.app (client) and pwos.app (advisor). Subprocessors page reference added.
- **v3** (March 19, 2026) — Prior baseline. Superseded in full by v3.2.

Questions?

If you have any questions about this privacy notice, please contact us at privacy@protocolwealthllc.com or security@protocolwealthllc.com, or reach us at:

Protocol Wealth, LLC Attn: Chief Compliance Officer (Adam Blumberg) 201 Milwaukee St., Suite 200 Denver, CO 80206 Phone: 720-383-4550

Protocol Wealth, LLC / SEC-Registered Investment Adviser / CRD #335298

Form ADV / Form ADV Part 2A / Form CRS / Terms of Service / Subprocessors / Disclosures