Privacy Policy

AI No Hype Clarity Systems with Signalproof

Last Revised: April 01, 2026
Effective: April 01, 2026

AI No Hype Clarity Systems with Signalproof cares about your privacy. We collect, use, store, and protect personal information only as needed to provide our websites, business systems, AI-supported tools, CRM services, training programs, consulting services, coaching services, memberships, workshops, digital products, and related services.

This Privacy Policy explains what information we collect, how we use it, how we protect it, when we may share it, and what rights and choices may be available to you.

For purposes of this Privacy Policy, "AI No Hype," "Clarity System," "Signalproof," "we," "our," or "us" refers to AI No Hype Clarity Systems with Signalproof, including its websites, funnels, landing pages, CRM systems, AI tools, training portals, memberships, events, coaching programs, communications, and services.

By using our websites, submitting a form, booking a session, purchasing a product or service, participating in a program, accessing our systems, or otherwise interacting with us, you agree to the practices described in this Privacy Policy.

For privacy-related questions, requests, or concerns, contact us at:

privacy@mail.ainohype.com

For support-related questions, contact:

support@mail.ainohype.com

Cookie Notice

We use cookies and similar technologies to improve your experience, support website functionality, understand site performance, support security, personalize content, and improve our Services.

You may be given the option to:

Accept All Cookies
Accept Essential Cookies Only
Reject Non-Essential Cookies

Rejecting non-essential cookies may prevent some non-essential features, analytics, personalization, or advertising tools from loading. Essential cookies may still be used where needed for website functionality, security, account access, checkout, consent management, or service delivery.

1. Who We Are

AI No Hype is the parent brand and practical AI philosophy.

Clarity System is the business operating ecosystem. It may include CRM infrastructure, workflow automation, proprietary AI-supported tools, LLM-powered workspaces, business dashboards, forms, calendars, funnels, pipelines, memberships, learning areas, and implementation support.

Signalproof is the training, framework, and adoption methodology inside the ecosystem. It supports clarity, communication, workflow discipline, execution habits, business focus, and practical AI adoption.

Our Services are designed to help business owners, operators, teams, creators, educators, coaches, consultants, local service businesses, martial arts studios, and other organizations use AI and systems with clarity, control, confidence, and disciplined execution.

2. Scope of This Privacy Policy

This Privacy Policy applies to information collected through:

- **Our websites and landing pages**
- **AI No Hype funnels and forms**
- **Clarity System accounts and workspaces**
- **Signalproof training, coaching, and assessment tools**
- **CRM systems and automation workflows**
- **Booking and calendar systems**
- **Email, SMS, phone, chat, and direct messages**
- **Webinars, workshops, live events, and cohort programs**
- **Payment and checkout pages**
- **Membership portals, LMS areas, and digital product access**

- **Client onboarding forms, discovery forms, and consultation requests**
- **Support requests and service communications**
- **Any other online or offline interaction connected to our Services**

This Privacy Policy does not apply to third-party websites, platforms, tools, or services that we do not control.

3. Information We Collect

We collect information so we can provide, operate, improve, secure, and personalize our Services.

The information we collect may include the following categories.

A. Personal Identifiers

We may collect:

- **Name**
- **Business name**
- **Email address**
- **Phone number**
- **Mailing address**
- **Billing address**
- **Username or account ID**
- **Social media profile links you provide**
- **Website URL**
- **IP address**
- **Device identifiers**
- **Other information that can identify you directly or indirectly**

B. Contact and Communication Information

We may collect information when you contact us or communicate with us, including:

- **Email messages**
- **Contact form submissions**
- **Chat messages**
- **SMS or text messages**
- **Phone call details**
- **Voicemail information**
- **Calendar booking details**

- **Consultation notes**
- **Support tickets**
- **Survey responses**
- **Feedback forms**
- **Direct messages through social platforms**

We may keep notes or records about what you asked, how we responded, and what next steps were requested or agreed upon.

C. Account-Related Information

If you create an account, join a program, purchase access, or use a system we provide, we may collect:

- **Account login information**
- **Account status**
- **User role or permissions**
- **Subscription level**
- **Products or services purchased**
- **Renewal or expiration dates**
- **Membership status**
- **Usage history**
- **Service preferences**
- **Support history**
- **Settings, permissions, and access logs**

D. Business and Operational Information

Because Clarity System and Signalproof are business-support systems, we may collect business-related information you provide, including:

- **Business goals**
- **Offers, products, or services**
- **Target audience**
- **Customer journey information**
- **Sales pipeline details**
- **CRM structure**
- **Lead follow-up process**
- **Marketing strategy**
- **Brand messaging**
- **Content strategy**
- **Workflow maps**
- **SOPs and internal processes**

- **Team roles and responsibilities**
- **Customer service processes**
- **Training materials**
- **Business documents, scripts, templates, or notes**
- **Pain points, bottlenecks, priorities, and implementation needs**

This information is used to help provide strategy, configuration, training, automation, implementation, coaching, and AI-supported workflow assistance.

E. CRM, Lead, and Customer Data

Some Clarity System packages may include CRM setup, automation, customer relationship management, pipeline tools, appointment tools, contact management, lead tracking, memberships, LMS tools, or learning systems.

Depending on your package and usage, CRM-related information may include:

- **Lead names**
- **Customer names**
- **Email addresses**
- **Phone numbers**
- **Appointment records**
- **Form responses**
- **Tags, notes, and pipeline stages**
- **Purchase history**
- **Membership access status**
- **Messages and follow-up history**
- **Customer service notes**
- **Internal workflow records**
- **Automation activity**
- **Calendar and booking data**

When we process CRM data for a client, we do so to provide the requested Services.

We do not sell client CRM contacts.

We do not use client CRM contacts for our unrelated marketing.

We do not contact your customers on our own behalf unless you authorize us to do so as part of a contracted service.

F. AI Tool and Workspace Information

If you use AI-supported features, proprietary LLM tools, AI workspaces, prompt systems, workflow assistants, or AI-enabled support tools, we may collect:

- **Prompts you submit**
- **Uploaded documents**
- **Generated outputs**
- **Workflow instructions**
- **Business context provided to the system**
- **AI workspace activity**
- **Tool usage history**
- **Error logs**
- **Performance logs**
- **Configuration data**
- **User feedback**

We use this information to provide AI-supported features, improve workflows, troubleshoot technical issues, support account functionality, and deliver Services.

G. Payment and Commercial Information

When you purchase a product, service, program, subscription, event, workshop, sprint, or consultation, we may collect:

- **Name**
- **Billing address**
- **Email address**
- **Phone number**
- **Product or service purchased**
- **Purchase date**
- **Subscription status**
- **Invoice records**
- **Payment confirmation**
- **Refund or dispute records**
- **Tax-related information where required**

Payment card information is generally processed by third-party payment processors. We do not intentionally store full payment card numbers on our own systems unless clearly disclosed and securely handled through an approved payment provider.

H. Training, Coaching, Quiz, and Assessment Information

Signalproof programs may include training, coaching, quizzes, worksheets, clarity sessions, progress reviews, implementation check-ins, and assessments.

We may collect:

- **Quiz answers**
- **Self-assessment responses**
- **Business clarity responses**
- **Coaching notes**
- **Implementation milestones**
- **Training progress**
- **Homework submissions**
- **Strategy session notes**
- **Workflow exercises**
- **Content planning answers**
- **Progress tracking information**

This information is used to provide training, improve your implementation, personalize coaching, and help you use the system effectively.

I. Website, Device, and Usage Information

When you use our websites, forms, funnels, platforms, or systems, we may automatically collect:

- **IP address**
- **Browser type**
- **Browser settings**
- **Device type**
- **Operating system**
- **Language preferences**
- **Referring pages**
- **Pages visited**
- **Time spent on pages**
- **Links clicked**
- **Forms opened or submitted**
- **Videos viewed**
- **Error data**
- **Cookie identifiers**
- **Device identifiers**
- **Approximate location based on IP address**
- **Date and time of activity**
- **Log files and metadata**

This information helps us improve performance, troubleshoot problems, protect our systems, understand user behavior, and improve our Services.

J. Supplemented Information

We may receive information from other sources, such as:

- **Public business directories**
- **Public websites**
- **Social media pages**
- **Referral partners**
- **Business databases**
- **Event registrations**
- **Advertising or analytics partners**
- **Third-party platforms you authorize**
- **Information provided by another person with your permission**

If you provide us personal information about another person, or if someone else provides us information about you, we will use that information only for the purpose for which it was provided or as otherwise allowed by law.

4. Sensitive Information

We do not intentionally request sensitive personal information unless it is necessary for a specific service, legal requirement, safety need, or client-authorized business purpose.

Sensitive information may include:

- **Social Security numbers**
- **Government identification numbers**
- **Financial account credentials**
- **Health information**
- **Biometric information**
- **Precise geolocation**
- **Information about minors**
- **Legal case details**
- **Highly confidential business records**
- **Trade secrets**
- **Employee records**
- **Regulated customer data**

Do not upload or submit sensitive information unless it is necessary, authorized, and appropriate for the Service you are using.

If your business involves regulated data, such as health, legal, financial, student, child, employee, or highly confidential business data, additional agreements, safeguards,

compliance reviews, or specialized terms may be required before we can process that information.

5. How We Use Information

We use information for the following purposes.

A. To Provide Our Services

We may use information to:

- **Deliver products, programs, memberships, and services**
- **Create and manage accounts**
- **Process purchases and subscriptions**
- **Book and manage consultations**
- **Provide coaching and training**
- **Configure CRM systems**
- **Build workflows and automations**
- **Deliver AI-supported tools**
- **Provide access to digital products**
- **Support memberships, courses, and learning systems**
- **Respond to service requests**
- **Provide customer support**
- **Manage onboarding and implementation**

B. To Build, Configure, and Support Clarity System

We may use information to:

- **Set up CRM pipelines**
- **Configure calendars**
- **Build forms and funnels**
- **Create workflows**
- **Connect automations**
- **Organize customer journeys**
- **Build dashboards**
- **Support internal knowledge systems**
- **Configure AI-supported workspaces**
- **Create SOPs, scripts, and templates**
- **Troubleshoot account or system issues**
- **Maintain service functionality**

C. To Deliver Signalproof Training and Adoption Support

We may use information to:

- **Help clarify offers, audiences, workflows, and priorities**
- **Support implementation discipline**
- **Develop business maps and operating cadences**
- **Create prompt libraries and workflow playbooks**
- **Support coaching, mentoring, and training**
- **Track progress during sprints, cohorts, or programs**
- **Improve communication, organization, and execution habits**
- **Help users apply AI in practical business contexts**

D. To Communicate With You

We may use information to contact you about:

- **Bookings and appointments**
- **Purchases and subscriptions**
- **Account access**
- **Service updates**
- **Training reminders**
- **Program announcements**
- **Support requests**
- **Billing matters**
- **Security alerts**
- **Policy updates**
- **Marketing messages**
- **Offers we believe may be relevant to you**

These communications may occur by:

- **Email**
- **SMS or text message**
- **Phone call**
- **Automated phone call, where permitted**
- **Direct message**
- **Chat**
- **Postal mail**
- **In-platform notification**

You do not need to consent to marketing communications as a condition of purchasing our Services.

E. To Improve, Update, and Enhance Services

We may use information to:

- **Improve website performance**
- **Improve system functionality**
- **Analyze user behavior**
- **Understand what services are most relevant**
- **Diagnose technical problems**
- **Identify needed enhancements**
- **Improve training materials**
- **Improve AI-supported workflows**
- **Improve support and onboarding**
- **Develop new offers, products, and services**

When possible, we use aggregated or de-identified information for improvement and analytics.

F. To Protect Our Business, Users, and Systems

We may use information to:

- **Detect and prevent fraud**
- **Monitor abuse or misuse**
- **Protect accounts**
- **Secure systems**
- **Investigate suspicious activity**
- **Prevent unauthorized access**
- **Enforce agreements**
- **Protect intellectual property**
- **Protect the safety of users, clients, staff, or the public**

G. To Meet Legal and Business Obligations

We may use information to:

- **Comply with laws and regulations**
- **Maintain tax and accounting records**
- **Respond to legal requests**
- **Resolve disputes**
- **Enforce contracts**
- **Process refunds or chargebacks**
- **Maintain business records**

- **Cooperate with lawful investigations**
- **Protect legal rights**

6. AI, LLM, and Private Business Data Policy

Because AI No Hype Clarity Systems with Signalproof includes AI-supported tools and implementation support, this section explains how we approach AI-related data.

A. Private Business Data

We treat your private business data, CRM data, customer records, strategy documents, SOPs, scripts, workflows, uploaded files, and internal materials as confidential business information.

We do not claim ownership over your private business content.

We use your private business content only as needed to provide the Services you requested.

B. Private-System Posture

AI No Hype Clarity System is designed around a private-system posture.

That means private business information, CRM data, customer records, internal strategy materials, and uploaded business documents are intended to remain within the controlled systems used to provide your requested Services.

We do not intentionally submit your private CRM data, customer lists, business records, uploaded files, or confidential internal materials into public consumer chatbot interfaces for unrelated use.

Examples of public consumer chatbot interfaces may include public versions of tools such as ChatGPT, Claude, Gemini, Grok, or similar services.

Where private AI infrastructure, APIs, secure LLM services, CRM systems, automation providers, hosting services, or third-party technical providers are used to deliver a requested Service, processing is limited to service delivery, system functionality, troubleshooting, support, security, or improvement, subject to applicable vendor terms and safeguards.

C. No Public Model Training Permission

We do not intentionally use your private business data, CRM contacts, uploaded documents, SOPs, internal workflows, or confidential materials to train public AI models.

If a specific tool, vendor, or AI provider has its own data-processing terms, those terms may apply to the technical processing needed to deliver the Service.

D. No Government or Public Institution Sharing Except When Required

We do not voluntarily share your private business data, CRM records, customer lists, uploaded files, or confidential materials with government institutions or public institutions for unrelated purposes.

We may disclose information only if required by law, legal process, court order, subpoena, regulatory obligation, or to protect rights, safety, security, or property.

Where legally permitted and appropriate, we may take reasonable steps to notify you before disclosing information in response to legal process.

E. User Responsibility

You are responsible for ensuring that any data, documents, files, customer information, employee information, or business materials you upload or provide are information you have the right to use, process, and share with us for service delivery.

You should not submit confidential, regulated, sensitive, or third-party information unless you have the proper authority and legal basis to do so.

F. AI Outputs Are Supportive, Not Professional Advice

AI-supported outputs may help with drafting, planning, brainstorming, workflow design, strategy, organization, and business support.

AI outputs are not a substitute for legal, tax, financial, medical, insurance, compliance, mental health, or other licensed professional advice.

You are responsible for reviewing, verifying, and approving any AI-supported output before using it in your business.

7. How We Share Information

We may share information with trusted third parties only as needed to operate our business, deliver Services, comply with law, or protect rights and security.

A. Service Providers

We may share information with providers that help us operate our Services, such as:

- **CRM platforms**
- **Website hosting providers**
- **Funnel and landing page providers**
- **Payment processors**
- **Email service providers**
- **SMS and phone providers**
- **Calendar and booking tools**
- **Automation platforms**
- **AI infrastructure providers**
- **Cloud storage providers**
- **Analytics providers**
- **Advertising platforms**
- **Customer support tools**
- **Course, membership, or LMS platforms**
- **Developers, contractors, and technical support providers**
- **Legal, accounting, bookkeeping, tax, or compliance professionals**

These providers are authorized to use information only as needed to provide services to us or to you, subject to their own applicable legal and contractual obligations.

B. Business Partners and Integrated Services

Some Services may allow integrations with third-party platforms or partners.

If you choose to connect or use a third-party integration, information may be shared as needed to perform the requested integration or function.

If we collect information through a co-branded offer, joint program, affiliate campaign, or partner service, we will identify the relevant parties where appropriate and describe available choices when required.

C. Client-Authorized Sharing

We may share information when you authorize or direct us to do so, including when:

- **You ask us to connect a tool**
- **You request migration of data**
- **You authorize a contractor or team member**
- **You ask us to send information to a third party**
- **You request a report, export, or integration**
- **You approve a case study, testimonial, or public result**

D. Legal, Regulatory, and Safety Reasons

We may disclose information when we believe it is necessary or appropriate to:

- **Comply with law**
- **Respond to subpoenas, court orders, or legal process**
- **Cooperate with lawful government or law enforcement requests**
- **Protect our rights, property, or safety**
- **Protect the rights, property, or safety of users, clients, staff, or the public**
- **Prevent fraud, abuse, or security incidents**
- **Enforce contracts or terms**
- **Resolve disputes**

When legally permitted and appropriate, we may take reasonable steps to notify you before disclosing your information in response to legal process.

E. Business Transfers

If we are involved in a merger, acquisition, financing, reorganization, sale of assets, bankruptcy, or transfer of business operations, information may be transferred as part of that transaction.

Any successor organization will be expected to honor this Privacy Policy or provide notice of changes as required by law.

8. What We Do Not Sell

We do not sell your private business data.

We do not sell your CRM contacts.

We do not sell your uploaded documents.

We do not sell your private customer lists.

We do not use your CRM data for our unrelated marketing.

We do not share your confidential business information publicly without permission.

Some advertising or analytics activities may be considered "sharing" under certain privacy laws if they involve cross-context behavioral advertising. Where required, we will provide opt-out options.

9. Cookies, Pixels, Analytics, and Similar Technologies

We may use cookies, pixels, tags, scripts, web beacons, device identifiers, local storage, and similar technologies.

These technologies may help us:

- **Keep websites functional**
- **Remember user preferences**
- **Support account login**
- **Secure forms and checkout**
- **Analyze site traffic**
- **Measure campaign performance**
- **Understand visitor behavior**
- **Improve website design**
- **Personalize content**
- **Deliver or measure advertisements**
- **Prevent fraud or abuse**

A. Essential Cookies

Essential cookies are necessary for website functionality, security, checkout, forms, consent management, login, and service delivery.

These may load even if you reject non-essential cookies.

B. Analytics Cookies

Analytics cookies help us understand how users interact with our websites, pages, forms, and content.

We may use analytics tools such as Google Analytics or similar providers.

Analytics providers may collect information such as pages visited, time on site, browser type, device type, referring pages, and approximate location based on IP address.

C. Advertising and Retargeting Cookies

We may use advertising or retargeting tools to present relevant offers or measure marketing performance.

Third-party advertising partners may use cookies or similar technologies to understand browsing behavior and measure advertising effectiveness.

Where required, you may opt out of sale, sharing, or targeted advertising through cookie settings, browser tools, or links provided on our website.

D. Cookie Choices

You may control cookies through:

- **Our cookie banner or cookie settings, where available**
- **Your browser settings**
- **Third-party opt-out tools**
- **Platform advertising preferences**
- **Device privacy settings**

Blocking cookies may limit some website features.

10. Website Analytics

We may use analytics tools to collect information about website and platform usage, including:

- **Pages visited**
- **Links clicked**
- **Time spent on pages**
- **Prior website visited**
- **Browser type**
- **Operating system**
- **Device type**
- **Network information**
- **IP address**

- **Form interactions**
- **Error data**

We use this information to improve website performance, user experience, service offerings, marketing strategy, and system reliability.

Analytics providers may store information on servers located in the United States or other countries and may process information according to their own privacy policies.

11. Targeted Advertising

We may partner with third-party advertising platforms to deliver ads, measure campaigns, and understand whether marketing is effective.

These partners may use cookies, pixels, or similar technologies to collect information about activity on our websites and other websites.

You may still receive generic advertising even if you opt out of targeted advertising.

Where applicable, we will provide a "Do Not Sell or Share My Personal Information" or similar opt-out mechanism.

12. Imported Contacts and Client Lists

If you use a Service that allows you to upload, import, or manage contacts, such as CRM, email marketing, SMS, appointment reminders, or pipeline automation, we will use those contacts only to provide the requested Service.

You are responsible for ensuring that:

- **You have permission to contact imported contacts**
- **Your contact lists were collected lawfully**
- **Your messages comply with applicable email, SMS, telemarketing, privacy, and consent laws**
- **Your business has appropriate unsubscribe, opt-out, and consent processes**

If someone believes their information was provided to us improperly, they may contact us at:

privacy@mail.ainohype.com

For support assistance, contact:

support@mail.ainohype.com

13. Email, SMS, Phone, and Automated Communications

We may contact you directly or through service providers by:

- **Email**
- **SMS or text message**
- **Phone call**
- **Voicemail**
- **Automated phone call, where permitted**
- **Automated text message, where permitted**
- **Direct message**
- **In-platform notification**
- **Postal mail**

We may contact you about:

- **Services you requested**
- **Account access**
- **Appointments**
- **Purchases**
- **Program updates**
- **Billing**
- **Support**
- **Security**
- **Policy updates**
- **Marketing and offers**

You may unsubscribe from marketing emails by using the unsubscribe link in the email.

You may opt out of SMS messages by replying STOP, where supported.

You may still receive transactional, legal, billing, security, or service-related messages even after opting out of marketing communications.

For support questions, contact:

support@mail.ainohype.com

For privacy requests, contact:

privacy@mail.ainohype.com

14. Third-Party Websites and Platforms

Our websites, funnels, emails, or Services may contain links to third-party websites, platforms, tools, or services.

We are not responsible for the privacy practices, security, policies, or content of third-party websites or platforms.

You should review the privacy policy of any third-party service you use.

15. International Transfers

Our Services are primarily operated from the United States.

If you access our Services from outside the United States, your information may be transferred to, stored in, or processed in the United States or other countries where we or our service providers operate.

Those countries may have data protection laws that differ from the laws in your location.

Where required, we rely on lawful transfer mechanisms, which may include:

- **Your consent**
- **Contractual necessity**
- **Standard contractual clauses**
- **Adequacy decisions**
- **Approved transfer mechanisms**
- **Vendor participation in recognized data transfer frameworks, where applicable**

16. EU-U.S., UK-U.S., and Swiss-U.S. Data Privacy Framework

The former Privacy Shield Frameworks are no longer the current controlling framework for EU-U.S. transfers.

The current official framework is the EU-U.S. Data Privacy Framework, with related UK and Swiss extensions where applicable.

We will only claim certification under the Data Privacy Framework if we are officially certified and listed as a participating organization.

If we are not certified, we may rely on other lawful transfer mechanisms, such as standard contractual clauses or vendor transfer mechanisms.

17. Data Security

We use reasonable administrative, technical, and organizational safeguards designed to protect information from unauthorized access, loss, misuse, alteration, disclosure, or destruction.

Security measures may include:

- **Password-protected systems**
- **Permission-based access**
- **Limited internal access**
- **Account role controls**
- **Vendor access controls**
- **Secure payment processors**
- **Encryption where appropriate**
- **Secure hosting providers**
- **Monitoring for misuse or suspicious activity**
- **Internal confidentiality expectations**
- **Contractor and vendor access limits**
- **Backup, recovery, and continuity practices where appropriate**

No online system, transmission method, or storage system is completely secure.

You are responsible for protecting your login credentials, devices, passwords, and account access.

If you believe your account or information has been compromised, contact us immediately at:

privacy@mail.ainohype.com

For technical or account support, contact:

support@mail.ainohype.com

18. Data Retention

We retain information only as long as reasonably necessary for the purposes described in this Privacy Policy.

Retention may be based on:

- **The type of information**
- **The nature of the Service**
- **Account status**
- **Contractual obligations**
- **Legal requirements**
- **Tax and accounting obligations**
- **Security needs**
- **Dispute resolution**
- **Fraud prevention**
- **Business recordkeeping**
- **Client support needs**

We may retain information for legitimate business or legal purposes, including:

- **Providing requested Services**
- **Maintaining accurate business and financial records**
- **Preserving legal or contractual rights**
- **Resolving disputes**
- **Enforcing agreements**
- **Complying with laws**
- **Protecting systems and users**

When information is no longer needed, we may delete, anonymize, archive, or securely dispose of it.

19. How You Can Access, Update, or Delete Your Information

Depending on your location and the Services you use, you may have the right to:

- **Access your personal information**
- **Correct inaccurate information**
- **Delete certain information**
- **Request a copy of your information**
- **Restrict certain processing**
- **Object to certain processing**
- **Opt out of marketing communications**

- **Opt out of sale or sharing, where applicable**
- **Update account settings**
- **Close or deactivate an account, where available**

To make a privacy request, contact:

privacy@mail.ainohype.com

We may need to verify your identity before fulfilling certain requests.

We may deny or limit requests where allowed by law, including where information is needed to:

- **Provide Services**
- **Complete transactions**
- **Maintain security**
- **Prevent fraud**
- **Comply with legal obligations**
- **Maintain business records**
- **Resolve disputes**
- **Enforce agreements**

For account or service help, contact:

support@mail.ainohype.com

20. California Privacy Notice

This section applies to California residents where the California Consumer Privacy Act, as amended by the California Privacy Rights Act, applies.

In the past 12 months, we may have collected the following categories of personal information:

Category	Examples	Purpose
Identifiers	**Name, email, phone, business name, IP address, account ID**	**Account creation, communication, service delivery, support, billing**

Customer Records	**Billing details, purchase history, contact details**	**Purchases, subscriptions, invoices, service records**
Commercial Information	**Products purchased, services used, subscription status**	**Fulfillment, support, analytics, business records**
Internet or Network Activity	**Pages visited, device data, cookies, links clicked**	**Analytics, security, website improvement, marketing**
Geolocation Data	**Approximate location from IP address**	**Security, analytics, personalization**
Professional or Business Information	**Job title, business goals, workflows, CRM needs**	**Service delivery, coaching, implementation, training**
Audio, Electronic, or Similar Information	**Calls, messages, recordings, webinar participation, where applicable**	**Support, training, quality, documentation**
Inferences	**Service interests, training needs, business priorities**	**Personalization, recommendations, service improvement**
Sensitive Personal Information	**Only if submitted and necessary**	**Service delivery, legal compliance, security**

Sources of Personal Information

We may collect personal information from:

- **You directly**
- **Your business or organization**
- **Website forms**
- **Booking pages**
- **Purchases**
- **Account registration**
- **CRM activity**
- **Uploaded documents**
- **Coaching or training sessions**
- **Emails, SMS, calls, and direct messages**
- **Public business sources**
- **Referral partners**
- **Analytics tools**
- **Service providers**
- **Advertising platforms**
- **Third-party integrations you authorize**

Purposes for Collection

We may collect and use personal information for:

- **Providing Services**
- **Processing payments**
- **Managing accounts**
- **Configuring CRM systems**
- **Delivering AI-supported tools**
- **Providing training and coaching**
- **Communicating with you**
- **Marketing and advertising**
- **Website analytics**
- **Security and fraud prevention**
- **Legal compliance**
- **Business operations**
- **Improving Services**

Disclosure of Personal Information

We may disclose personal information to:

- **Service providers**
- **Contractors**
- **Payment processors**
- **CRM and automation providers**
- **Analytics providers**
- **Advertising partners**
- **Cloud and hosting providers**
- **Legal and accounting professionals**
- **Business partners where authorized**
- **Government or legal authorities where required**

Sale or Sharing of Personal Information

We do not sell your private business data, CRM contacts, uploaded documents, or confidential client information.

We do not sell personal information in the traditional sense of exchanging it for money.

However, some analytics, advertising, or retargeting activities may be considered "sharing" under California privacy law if they involve cross-context behavioral advertising.

Where applicable, California residents may opt out of sale or sharing by contacting:

privacy@mail.ainohype.com

Subject line:

Do Not Sell or Share Request

California Privacy Rights

California residents may have the right to:

- **Know what personal information we collect**
- **Access personal information**
- **Request deletion**
- **Request correction**
- **Opt out of sale or sharing**
- **Limit use of sensitive personal information, where applicable**
- **Not be discriminated against for exercising privacy rights**

To exercise these rights, contact:

privacy@mail.ainohype.com

Subject line:

California Privacy Request

You may also designate an authorized agent to make a request on your behalf. We may require proof of authorization and identity verification.

21. Notice Regarding Sensitive Personal Information

We do not use sensitive personal information to infer characteristics about you unless permitted by law or necessary to provide the requested Service.

We do not intentionally collect sensitive personal information unless you provide it or it is necessary for a specific business, legal, security, or service purpose.

22. Nevada Privacy Rights

Nevada residents may have the right to opt out of certain sales of covered information.

We do not currently sell covered information as defined by Nevada law.

Nevada residents may submit requests to:

privacy@mail.ainohype.com

Subject line:

Nevada Privacy Request

23. EEA, UK, and Swiss Privacy Rights

If you are located in the European Economic Area, United Kingdom, or Switzerland, you may have certain rights under applicable data protection laws.

These may include the right to:

- **Access personal data**
- **Correct inaccurate personal data**
- **Request deletion**
- **Restrict processing**
- **Object to processing**
- **Request data portability**
- **Withdraw consent**
- **Lodge a complaint with a supervisory authority**

Where required, our legal bases for processing may include:

- **Consent**
- **Contractual necessity**
- **Legitimate interests**
- **Legal obligation**
- **Protection of rights and safety**

Examples of legitimate interests may include providing Services, improving systems, communicating with clients, preventing fraud, protecting security, and operating our business.

To exercise rights, contact:

privacy@mail.ainohype.com

24. Data Protection Authority

If you are located in the EEA, UK, or Switzerland and believe we process your personal data subject to GDPR or related privacy laws, you may have the right to contact your local data protection authority.

For UK residents, the supervisory authority is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
United Kingdom
Website: ico.org.uk
Phone: +44 303 123 1113

25. “Do Not Track” Signals

Some browsers allow users to send “Do Not Track” signals.

There is currently no consistent industry standard for responding to Do Not Track signals.

Like many websites, we may not alter our practices when we receive a Do Not Track signal.

Where required, we will honor legally recognized browser-based opt-out signals, global privacy controls, cookie preferences, or other required privacy signals.

26. Age Restrictions and Children’s Privacy

Our Services are intended for users who are at least 18 years old.

Our Services are not directed to children under 13.

We do not knowingly collect personal information directly from children under 13 without appropriate parental or legal consent.

Some clients, such as martial arts studios, schools, youth programs, training programs, family businesses, or membership organizations, may collect or store information about minors inside their own CRM systems.

In those cases, the client is responsible for obtaining proper consent and complying with applicable child privacy, parental consent, education, youth program, and data protection laws.

If you believe a child has provided personal information to us improperly, contact:

privacy@mail.ainohype.com

27. Live Events, Physical Activities, and Safety-Related Information

Some AI No Hype, Signalproof, partner, or client-related live events may include in-person activities, workshops, demonstrations, filming, physical exercises, workouts, stunts, transportation, outdoor activities, martial arts, or other higher-risk environments.

If an event includes physical activity or safety-sensitive participation, we may collect additional information such as:

- **Emergency contact information**
- **Participation forms**
- **Liability waivers**
- **Attendance records**
- **Accessibility needs**
- **Safety acknowledgments**
- **Medical or health-related information you voluntarily provide**

This information is used only to manage safety, participation, risk, legal compliance, event coordination, and emergency response.

Live events that include workouts, physical exercises, stunts, transportation, or outdoor activities may require an expanded event-risk section, waiver, or separate terms for that specific activity.

28. Testimonials, Case Studies, Screenshots, and Results

We may request permission to use testimonials, case studies, screenshots, success stories, metrics, or client results.

We will not publicly identify you, your business, your private data, your CRM records, your customer information, or your confidential business materials without permission.

If you provide a testimonial, review, or public comment, you grant us permission to use it for marketing, unless otherwise agreed in writing.

We may use anonymized or aggregated results to describe general outcomes without identifying you.

29. Intellectual Property and Client Content

You retain ownership of your private business content, customer lists, documents, workflows, SOPs, scripts, brand materials, and uploaded files unless a separate written agreement says otherwise.

By submitting content to us, you grant us permission to use that content only as needed to provide, configure, support, improve, or deliver the requested Services.

We retain ownership of our own intellectual property, including:

- **Signalproof frameworks**
- **Training materials**
- **Templates**
- **Prompts**
- **System designs**
- **Course materials**
- **Coaching materials**
- **Business methods**
- **Brand assets**
- **Written materials**
- **Proprietary workflows**
- **Internal tools**
- **Strategic frameworks**

Use of our Services does not transfer ownership of our intellectual property unless agreed in writing.

30. Security of Login Credentials

You are responsible for maintaining the confidentiality of your account login credentials.

You agree not to:

- **Share passwords without authorization**
- **Allow unauthorized users to access your account**
- **Circumvent system permissions**
- **Upload harmful code**
- **Misuse systems**
- **Access data that does not belong to you**
- **Attempt to reverse engineer or compromise the Services**

Notify us immediately if you believe your account has been compromised.

For urgent account or technical support, contact:

support@mail.ainohype.com

For privacy or data concerns, contact:

privacy@mail.ainohype.com

31. Changes to This Privacy Policy

We may update this Privacy Policy from time to time.

If we make changes, we will update the "Last Revised" and "Effective" dates.

If we make material changes, we may notify you by:

- **Posting a notice on our website**
- **Sending an email**
- **Displaying a notice in your account**
- **Updating this Privacy Policy**
- **Using another reasonable method**

Continued use of our Services after changes become effective means you accept the updated Privacy Policy.

32. Contact Us

If you have questions, concerns, requests, or complaints about this Privacy Policy, our privacy practices, or our Services, contact us at:

AI No Hype Clarity Systems with Signalproof
Attn: Privacy / Data Protection Officer
Privacy Email: privacy@mail.ainohype.com
Support Email: support@mail.ainohype.com
General Contact: contact@mail.ainohype.com
General Information: info@mail.ainohype.com
Website: https://ainohype.com

We will respond to privacy requests within a reasonable time and, where applicable, within the timeframe required by law.